

CRITICAL INFRASTRUCTURE PROTECTION  
IN SAUDI ARABIA: A CASE STUDY ON PETROCHEMICAL  
INDUSTRY PROTECTION AGAINST TERRORIST  
ATTACKS AT JUBAIL INDUSTRIAL CITY (JIC)

By

KHALED SHURAEM ALUTAIBI

A Thesis Presented to the  
DEANSHIP OF GRADUATE STUDIES  
In Partial Fulfillment of the Requirements  
For the Degree of

MASTER OF SCIENCE  
IN  
COMPUTER ENGINEERING

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS,

Dhahran, Saudi Arabia

JUNE 2009

**CRITICAL INFRASTRUCTURE PROTECTION IN SAUDI  
ARABIA: A CASE STUDY ON PETROCHEMICAL INDUSTRY  
PROTECTION AGAINST TERRORIST ATTACKS AT JUBAIL  
INDUSTRIAL CITY (JIC)**

BY

**KHALED SHURAEM ALUTAIBI**

A Thesis Presented to the  
DEANSHIP OF GRADUATE STUDIES

**KING FAHD UNIVERSITY OF PETROLEUM & MINERALS**  
DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the  
Requirements for the Degree of

**MASTER OF SCIENCE**  
In  
**COMPUTER ENGINEERING**

**JUNE 2009**

# KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN 31261, SAUDI ARABIA

## DEANSHIP OF GRADUATE STUDIES

This thesis, written by **KHALED SHURAEM ALUTAIBI** under the direction of his thesis advisor and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE IN COMPUTER ENGINEERING.

### Thesis Committee

  
Dr. Lahouari Ghouti (Chairman)


  
Dr. Lahouari Cheded (Member)

  
Dr. Tarek Sheltami (Member)

  
Dr. Malick M. Ndiaye (Member)

  
Dr. Hamdi Yahyaoui (Member)

  
Dr. Adnan A. Gutub  
Department Chairman

  
Dr. Salam A. Zummo  
Dean of Graduate Studies

  
Date



## **ACKNOWLEDGEMENTS**

First and foremost, I would like to express my deep appreciation to Dr. Lahouari Ghouti, my adviser. He has the soul of a mentor, exceptionally generous in sharing his knowledge and experiences. I will never forget the many weekend afternoons we spent together reviewing what we have accomplished; discussing what could have been done better. I am grateful to his advices and guidance throughout this research.

I would like also to thank my thesis committee members Dr. Lahouari Cheded, Dr. Tarek Sheltami, Dr. Malick M. Ndiaye and Dr. Hamdi Yahyaoui for their sincere guidance and advice.

I would like to express my thanks to Professor Apostolakis and his team at MIT for their previous work in this area of research. I really appreciate for Prof. Apostolakis his quick responses in answering my questions and his generosity in sharing his latest researches.

Also, I thank all my friends who I always look to them with great fondness.

As always I thank my parents for their love and prayers. Also, I thank my brothers and sisters who gave all the support. I thank them for all they have done for me.

Finally, I am deeply indebted to my wife, my daughter Joody and my son Naif, for their love, patience, understanding and support.

KFUPM, JUNE 2009

Khaled Sh. Alutaibi

## Table of Contents

Acknowledgements .....	IV
List of Figures .....	IX
List of Tables .....	X
Thesis Abstract (English) .....	XII
Thesis Abstract (Arabic) .....	XIII
<b>Chapter One: Introduction .....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Defining the Problem .....	4
1.3 Purpose of Research .....	5
1.4 Rationale behind the Study .....	5
1.5 Research Contributions .....	7
1.6 Structure of this Thesis .....	9
<b>Chapter Two: Literature Review .....</b>	<b>10</b>
2.1 Introduction .....	10
2.2 The Relationship between Network Theory and CIP .....	12
2.3 CI Characteristics .....	20
2.4 Dependency .....	23
2.5 Interdependency .....	25
2.5.1 Physical Interdependency .....	26
2.5.2 Cyber Interdependency .....	26
2.5.3 Geographic Interdependency .....	27
2.5.4 Logical Interdependency .....	27
2.6 CIP Case Studies .....	28
2.6.1 USA .....	28
2.6.2 Canada .....	29
2.6.3 The United Kingdom .....	31
2.6.4 Australia .....	32
2.6.5 Germany .....	33
2.7 CI Interdependencies Modeling .....	33

2.7.1	A Screening Methodology for the Identification and Ranking of CIs Vulnerabilities due to Terrorism.....	34
2.7.2	Inoperability Input-Output Model for Interdependent Infrastructure .....	36
2.7.3	Agent-Based Model.....	38
2.7.4	Cell-Channel Model.....	38
2.7.5	Network Models.....	39
<b>Chapter Three: Methodology Overview .....</b>		<b>40</b>
3.1	Overall Methodology .....	40
3.2	Risk Analysis Model.....	45
3.2.1	Asset Assessment.....	46
3.2.2	Threat Assessment .....	47
3.2.3	Vulnerability Assessment .....	48
3.2.4	Identify Susceptibility to Different Threats .....	49
3.2.5	Risk Assessment .....	51
3.2.6	Identification of Countermeasure Options (Risk Management) .....	51
3.3	Location-based Production Loss Calculation (LPLC) .....	52
3.4	Proposed Methodology.....	54
<b>Chapter Four: Petrochemical Industry at JIC Case Study .....</b>		<b>57</b>
4.1	Background.....	57
4.2	Petrochemical Industry CI .....	58
4.3	Petrochemical Industry at JIC .....	59
4.4	JIC Value Tree and User Performance Index (PI) Assessment.....	61
4.4.1	Step 1: structuring the objectives .....	63
4.4.2	Step 2: determine appropriate performance measures .....	65
4.4.3	Step 3: weighing objectives and performance measures.....	67
4.4.4	Step 4: assessing utility functions of PMs.....	73
4.4.5	Step 5: performing consistency checks .....	76
4.5	Network Analysis .....	77
4.5.1	Production Minimum Cut Set (PMCS) for Node .....	77
4.5.2	Production Minimum Cut Set (PMCS) for Link.....	79
4.5.2.1	Scenarios types .....	80

4.5.2.1.1	<i>Terrorist attack scenarios</i> .....	80
4.5.2.1.2	<i>Machine failure scenarios</i> .....	82
4.6	Performance Index (PI) calculation for PMCS for machine failure and terrorist attack scenarios .....	84
4.7	Results and Analysis .....	86
4.8	Application of LPLC to Terrorist Attacks .....	89
4.9	Resources Allocation to Reduce the Overall Risk .....	95
Chapter Five: Conclusion .....		97
5.1	Conclusion .....	97
5.2	Future Work .....	97
Bibliography .....		98
Appendix A .....		105
Appendix B .....		107
Appendix C .....		108
Appendix D .....		113
Appendix E .....		127
Appendix F .....		130

## List of Figures

FIGURE 1-1 BASIC CRITICAL INFRASTRUCTURE PROTECTION PROCESS [7] .....	3
FIGURE 1-2 CONNECTIVITY AMONG PETROCHEMICAL FACTORIES AT JIC. ....	6
FIGURE 2-1 DIAGRAM OF GRAPH $G$ .....	14
FIGURE 2-2 DIGRAM OF DIGRAPH $D$ .....	16
FIGURE 2-3 DIAGRAM FOR DIGRAPH OF PETROCHEMICAL NETWORK AT JIC.....	18
FIGURE 2-4 EXAMPLES OF ELECTRIC POWER INFRASTRUCTURE DEPENDENCIES [26]. ....	24
FIGURE 2-5 EXAMPLE OF CI INTERDEPENDENCIES [26].....	25
FIGURE 3-1 PROPOSED VALUE TREE FOR PETROCHEMICAL FACTORIES AT JIC.....	43
FIGURE 3-2 RISK ANALYSIS MODEL [10]. ....	46
FIGURE 3-3 AREA COVERAGE OF TARGETED ZONES .....	53
FIGURE 3-4 PETROCHEMICAL FACTORIES IN JIC. ....	55
FIGURE 4-1: MAP OF KINGDOM OF SAUDI ARABIA.....	59
FIGURE 4-2: COMPONENTS OF SAUDI NON-OIL EXPORTS [73].....	60
FIGURE 4-3 JIC VALUE TREE.....	65
FIGURE 4-4 EXAMPLE OF DM1'S RELATIVE IMPORTANCE ASSESSMENT.....	69
FIGURE 4-5 CONSTRUCTED WEIGHT OF THE VALUE TREE FOR DM1. ....	70
FIGURE 4-6 PMCS ALGORITHM FOR NODES. ....	78
FIGURE 4-7 PMCS ALGORITHM FOR LINK.....	79
FIGURE 4-8 SCENARIO 1 LOCATION. ....	81
FIGURE 4-9 SCENARIO 2 LOCATION. ....	81
FIGURE 4-10 SCENARIO 3 LOCATION. ....	82
FIGURE 4-11 MACHINE FAILURE, SCENARIO 1, LOCATION. ....	83
FIGURE 4-12 MACHINE FAILURE, SCENARIO 2, LOCATION. ....	83
FIGURE 4-13 MACHINE FAILURE, SCENARIO 3, LOCATION. ....	84
FIGURE 4-14 VULNERABILITY OF MACHINE FAILURE SCENARIOS FOR NODES AT JIC. ....	87
FIGURE 4-15 VULNERABILITY OF MACHINE FAILURE SCENARIOS FOR LINKS AT JIC. ....	87
FIGURE 4-16 VULNERABILITY OF TERRORIST ATTACK SCENARIOS FOR NODES AT JIC.....	87
FIGURE 4-17 VULNERABILITY OF TERRORIST ATTACK SCENARIOS FOR LINKS AT JIC.....	88
FIGURE 4-18 GRAPHICAL REPRESENTATION OF THE VULNERABILITIES OF JIC TO MECHANICAL FAILURE.....	88
FIGURE 4-19 GRAPHICAL REPRESENTATION OF THE VULNERABILITIES OF JIC TO TERRORIST ATTACK.....	89
FIGURE 4-20 SCENARIO 1 WITH LPLC ZONES.....	90
FIGURE 4-21 SCENARIO 2 WITH LPLC ZONES.....	90
FIGURE 4-22 SCENARIO 3 WITH LPLC ZONES.....	91



## List of Tables

TABLE 2-1 INCIDENCE MATRIX FOR GRAPH G.....	15
TABLE 2-2 INCIDENCE MATRIX N (D) FOR DIGRAPH D .....	16
TABLE 2-3 INCIDENCE MATRIX OF PETROCHEMICAL INDUSTRY NETWORK AT JIC. ....	19
TABLE 3-1: PRELIMINARY CONSTRUCTED SCALE FOR PHYSICAL PROPERTY DAMAGE. ....	44
TABLE 3-2: AHP COMPARISON SCALE [61].....	44
TABLE 3-3: PRELIMINARY CONSTRUCTED SCALE FOR PHYSICAL PROPERTY DAMAGE WITH WIEGHT. ....	45
TABLE 3-4 THREAT ASSESSMENT SCINARIOS FOR JIC .....	47
TABLE 3-5 SUSCEPTIBILITY CATEGORIES. ....	48
TABLE 3-6 VULNERABILITY CATEGORIES [10]. ....	48
TABLE 3-7 VULNERABILITY CATEGORIES DESCRIPTION [10]. ....	49
TABLE 3-8 SUSCEPTIBILITY CATEGORIES FOR MECHANICAL FAILURES. ....	50
TABLE 3-9 SUSCEPTIBILITY CATEGORIES FOR MALEVOLENT ACTIONS.....	51
TABLE 3-10 LPLC ZONES.....	54
TABLE 4-1 INPUT AND OUTPUT QUANTITY FOR JIC FACTORIES. ....	62
TABLE 4-2 MAIN OBJECTIVES PROPOSED FOR DECISION MAKERS. ....	64
TABLE 4-3 CONSTRUCTED SCALES FOR SAFETY AND HEALTH .....	66
TABLE 4-4 CONSTRUCTED SCALES FOR IMAGE .....	66
TABLE 4-5 CONSTRUCTED SCALES FOR ECONOMIC .....	67
TABLE 4-6 CONSTRUCTED SCALES FOR ENVIRONMENT .....	67
TABLE 4-7 INITIAL CONSTRUCTED WEIGHT OF THE VALUE TREE FOR THE FIVE DECISION MAKERS.....	70
TABLE 4-8 DM1’S INITIAL MATRIX OF COMPARISONS.....	71
TABLE 4-9 DM1’S RANKING OF OBJECTIVES AND WEIGHTS.....	71
TABLE 4-11 DM3’S RANKING OF OBJECTIVES AND WEIGHTS.....	72
TABLE 4-12 DM4’S RANKING OF OBJECTIVES AND WEIGHTS.....	72
TABLE 4-13 DM5’S RANKING OF OBJECTIVES AND WEIGHTS.....	72
TABLE 4-14 CONSTRUCTED SCALES FOR SAFETY AND HEALTH WITH UTILITY VALUE.....	74
TABLE 4-15 CONSTRUCTED SCALES FOR IMAGE WITH UTILITY VALUE.....	75
TABLE 4-16 CONSTRUCTED SCALES FOR ECONOMIC WITH UTILITY VALUE. ....	75
TABLE 4-17 CONSTRUCTED SCALES FOR ENVIRONMENT WITH UTILITY VALUE. ....	75
TABLE 4-18 TERRORIST ATTACK SCENARIOS. ....	80
TABLE 4-19 MACHINE FAILURE SCENARIOS.....	82
TABLE 4-20 PMCS RAKED ACOORDING TO THIER VALUES FOR SCENARIO OF IN MACHINE FAILURE. ....	86
TABLE 4-23 LOSS CALCULATION DUE TO SCENARIO 1.....	92
TABLE 4-24 LOSS CALCULATION DUE TO SCENARIO 2. ....	93
TABLE 4-25 LOSS CALCULATION DUE TO SCENARIO 3. ....	94

TABLE 4-24 RESOURCE ALLOCATION TABLE.....95

TABLE 4-25 EXAMPLE OF RESOURCE ALLOCATION METHOD .....96

## THESIS ABSTRACT

**FULL NAME:** KHALED SHURAEM ALUTAIBI

**TITLE OF STUDY:** CRITICAL INFRASTRUCTURE PROTECTION IN SAUDI ARABIA: A CASE STUDY ON PETROCHEMICAL INDUSTRY PROTECTION AGAINST TERRORIST ATTACK AT JUBAIL INDUSTRIAL CITY (JIC)

**DEGREE:** MASTER OF SCIENCE

**MAJOR FIELD:** COMPUTER ENGINEERING

**DATE OF DEGREE:** JUNE 2009

Until recently, extremist groups had generally avoided industrial and economic targets. But nowadays, terrorists are changing their strategies and tactics by attacking petrochemical facilities which represents a threat to the physical security of petrochemical facilities. This Thesis proposes a methodology for the identification and prioritization of vulnerabilities in petrochemical industry at Jubail city (JIC) in Saudi Arabia. Existing methods are mostly based on an adaptation of the minimal-cut-set concept. We suggest that for both homogenous and heterogeneous Critical Infrastructures (CIs) a systematic scenario-based approach should be adopted.

We model CIs as interconnected digraphs. Production Minimum Cut Set (PMCS) technique is used to find cut sets for the CIs. Six scenarios are tested for both machine failure and terrorist attacks. All elements of CIs are prioritized based on vulnerabilities. The prioritization methodology is based on Multi-Attribute Utility Theory (MAUT). The impact of losing CI services is evaluated using a value tree that reflects the perceptions of five decision makers with different background. These results are provided to the decision maker for use in risk management. A location-based technique is used to help decision maker to calculate the loss due terrorist attacks. The methodology is illustrated through the presentation of the analysis conducted on petrochemical industry at JIC.

## ملخص الرسالة

الإسم : خالد بن شريم فايز العتيبي  
عنوان : حماية البنى التحتية في المملكة العربية السعودية: دراسة تطبيقية لحماية المنشآت البتروكيميائية في مدينة الجبيل الصناعية من خطر الهجمات الإرهابية  
الدرجة : ماجستير في العلوم  
التخصص : هندسة حاسب آلي  
تاريخ التخرج : يونيو 2009

إلى وقت قريب، لم تهتم الجماعات المتطرفة باستهداف المنشآت الصناعية والإقتصادية. و لكن لوحظ مؤخرا تغيرا في هذا التوجه إذ تقوم هذه الجماعات و الخلايا الإرهابية بتغيير الإستراتيجيات والتكتيكات و تبادر بمهاجمة المنشآت البتروكيميائية و يمثل هذا التوجه خطرا على الجانب الأمني لهذه المنشآت. تقدم هذه الأطروحة منهجية جديدة لتحديد مواطن الضعف و الأولويات لدى الصناعة البتروكيمياويات في مدينة الجبيل الصناعية في المملكة العربية السعودية. تعتمد معظم الحلول و الأساليب المستخدمة حاليا في هذا المجال على مفهوم الحد الأدنى من مجموعة القطع. ونقترح في هذه الرسالة استخدام منهجية نظامية معتمدة على السيناريوهات الممكنة لدراسة أمن البنى التحتية الأساسية المتجانسة وغير المتجانسة.

كما قمنا بتمثيل البنى التحتية الأساسية بواسطة رسم موجه مترابط (diagraph). تستخدم طريقة الحد الأدنى من مجموعة القطع للإنتاج لتحديد مجموعة القطع للبنى التحتية. كما تم اختبار ستة سيناريوهات تشمل حالات تعطل وحدات المنشآت و الهجمات الإرهابية على حد سواء. كذلك قمنا بتصنيف جميع الوحدات التابعة للبنى التحتية على أساس نقاط الضعف. و تقوم منهجية تحديد الأولويات على أساس نظرية المنفعة المتعددة السمات. يتم تقييم أثر فقدان خدمات إحدى البنى التحتية باستخدام شجرة قيم تعكس تصورات خمسة صناع القرار ذوي أولويات و اهتمامات مختلفة تماما. لقد عرضت نتائج هذه الدراسة على صناع القرار الخمسة من أجل استخدامها في إدارة المخاطر. ثم قمنا باستعمال تقنية معتمدة على الموقع لمساعدة صناع القرار في حساب الخسائر المتكبدة جراء تعطل وحدات المنشآت و الهجمات الإرهابية. تم توضيح المنهجية من خلال عرض التحليل المنفذ على الصناعة البتروكيمياويات في مدينة الجبيل الصناعية.

## **Chapter One: Introduction**

### **1.1 Introduction**

Saudi Arabia is the world's largest oil producer and exporter. It holds 25% of the world's proven oil reserves (261 billion barrels) and produces 12.5% of the world's oil production (about 9.0 million barrels a day) [1]. The stability of the global oil market depends on both the Kingdom's capacity to meet current shortages in oil supply and its ability to reassure the market that it will continue doing so in the future. Nowadays, the Kingdom is focusing on maintaining its ability to meet global oil demand and protect its key oil facilities.

Until recently, extremist groups had generally avoided industrial and economic targets. But nowadays, terrorists are changing their strategies and tactics by attacking petrochemical facilities and other national assets. This strategy change does not only present a threat to the physical security of petrochemical facilities, but it also aims to raise concern for the global energy market [1]. In 1988, a terrorist group called "Saudi Hezbollah" claimed responsibility for the bombing of Saudi petrochemical facilities [2]. Later on, in 2005, Saudi security forces discovered, in Dammam City, more than 60 hand grenades and pipe bombs, pistols, machine guns, RPGs, two barrels full of explosives and video equipment. The Saudi Minister of Interior was quoted as saying that the *al-Qaeda* cell had planned to attack Saudi oil and gas infrastructures. He added, "There

isn't a place that they could reach that they didn't think about," and insisted that al-Qaeda's ultimate goal has been to cripple the global economy [3].

Therefore, Saudi Arabia is currently facing challenges in dealing with the changing nature of terrorist attacks against its petrochemical resources. Oil fields and petrochemical plants, however, are large area targets and redundant facilities ensure that an attack on one would not cause a serious disruption in the entire production system. At any given time, there are approximately 25,000 to 30,000 troops protecting the Critical Infrastructures (CIs) in Saudi Arabia [4]. In 2005, the Saudi security budget was estimated to be 10 S.R. billion which includes funding several projects and initiatives to secure pipelines, oil fields and other energy terminals [4].

This thesis provides a study of the vulnerability assessment of petrochemical industries in Jubail Industrial City (JIC) in Saudi Arabia. Petrochemical industry is considered as one of the critical infrastructure (CI) sectors in many countries. In fact, there is no global definition for CI and each country determines its own critical categories independently of others. The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) defines CIs as those systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [5]. The CI list includes: agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy,

transportation, banking and finance, chemicals and hazardous materials, postal and shipping. Also, it includes “key assets” which are: national monuments and icons, nuclear power plants, dams and government facilities [6].

CI protection (CIP) refers to safeguarding the identified CIs and services from potential harm, including physical or electronic attacks [7]. It is widely agreed that the typical steps of CIP are vulnerability assessment, risk assessment and risk management [8]. These steps are illustrated in Figure 1.1 [7].

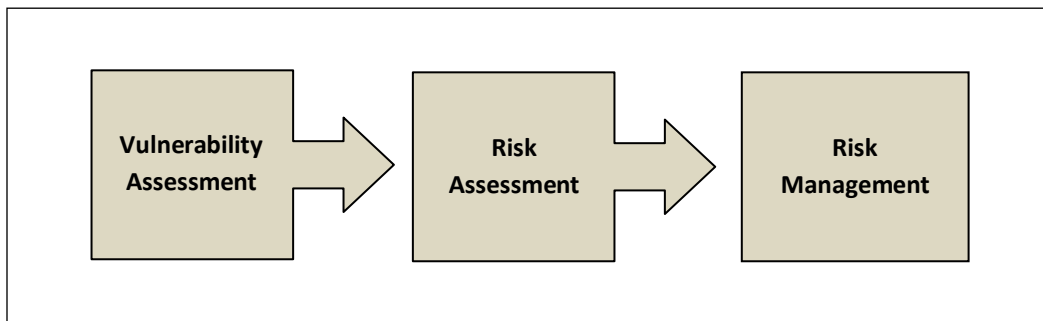


Figure 1-1 Basic Critical Infrastructure Protection Process [7]

Today, CIP gets more importance as a result of recent global events, including 9/11, 7/7 and the Bali bombings among others. Although CIP has been a global concern since the Cold War, It has regained more exposure since the occurrence of the above-mentioned incidents [8]. Also, the increased use of the Internet and Communication Technologies has amplified the risks to CIs [9]. These technologies have enabled easier data exchange and simplified the ability to transmit data, thus lightening the risks posed to the CI's.

## **1.2 Defining the Problem**

Government officials and industry observers agree that petrochemical sectors are a preferred target for terrorists. This point of consensus is based on several reasons:

1. Many of the industry's facilities are extremely vulnerable to attacks because of poor or lacking security. It is commonly believed that even unsophisticated strikes on such facilities would have a high probability of success.
2. Petrochemical sites are located within highly dense residential areas. Therefore, successful attacks on these facilities could destroy the lives of several thousand people over several regions.
3. A petrochemical plant attack could have devastating impacts on the local economy because many other industries are extremely dependent on the petrochemical industry for the supply of their raw materials.
4. Petrochemical facilities are often clustered together in industrial districts or near shipping ports. Therefore, an attack on one of these facilities could trigger a reaction chain of explosions at nearby plants and have a disastrous impact on trade and economy.
5. Terrorists may strike petrochemical sites to send a symbolic message. Many believe that this rationale was the primary reason behind the thwarted attacks on the White House/U.S. Capitol and the successful one on the Pentagon.
6. Most petrochemical sites have not yet implemented adequate protection measures to prevent or respond to terrorist attacks.



### **1.3 Purpose of Research**

In this thesis, we will assess the vulnerability assessment of petrochemical CIs in JIC in the Eastern Province of Saudi Arabia to potential attacks. The following issues will be addressed:

1. Suitability of the Network/Critical Node Analysis process to analyze the vulnerabilities of the petrochemical sector.
2. Investigation of the usability of the scenario-based approach, proposed by Apostolakis and Lemon [2], in revealing the CIs' vulnerabilities and allocating the available resources based on deployment costs. The scenario will be applied on a real case presented by some selected petrochemical plants in JIC (see Figure 1-2).
3. Provision of a heightened awareness and an informed guidance to help Saudi security forces and concerned stake holders to effectively deal with and contain attacks to the CI in the Saudi petrochemical industry.
4. Extension of the thesis findings and recommendations to other critical sectors in Saudi Arabia and provide a platform for such ambitious plans.

### **1.4 Rationale behind the Study**

Following the momentum of the security efforts exerted by the Saudi government in the wake of the 9/11 events and the observations made on the structure of the petrochemical industries located in JIC, the need to conduct effective vulnerability

assessments in the protection of the CIs hosted at JIC and other industrial locations became even stronger. Moreover, the following obvious facts provide further incentives for the intended research:

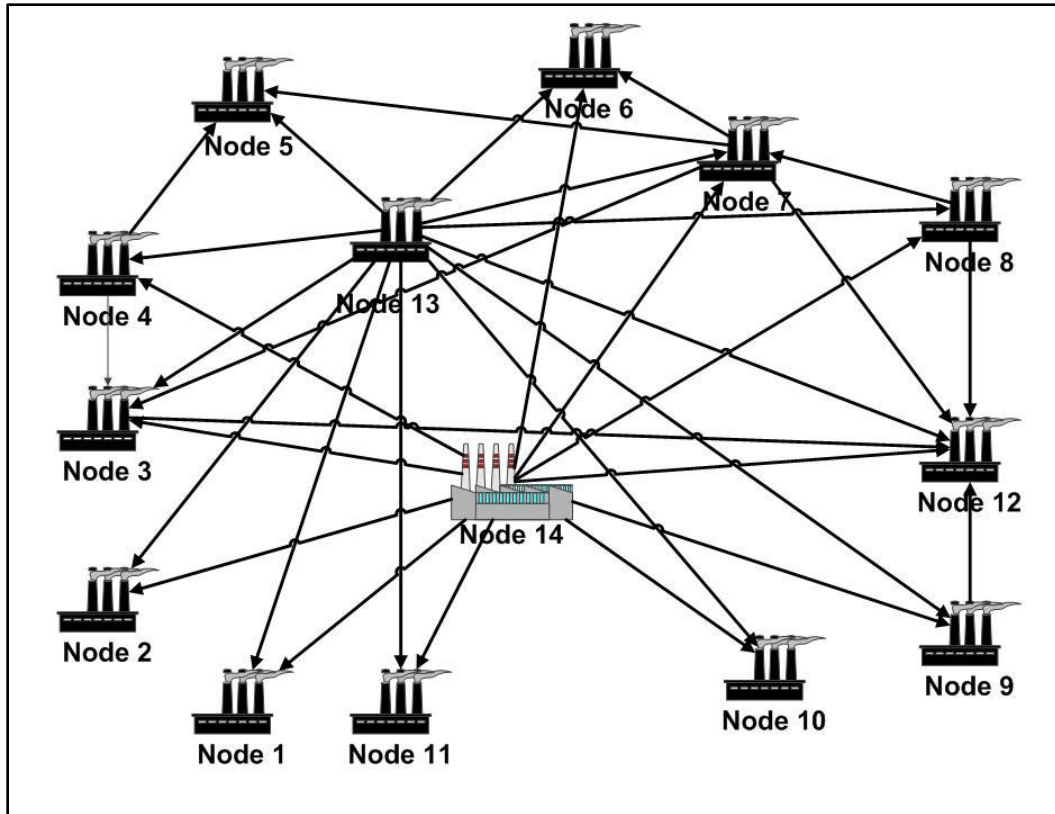


Figure 1-2 Connectivity among petrochemical factories at JIC.

1. The unequivocal and almost complete dependence of the Saudi economy on the petrochemical industry in general and the industries hosted at JIC in particular.
2. Based on the current configuration of JIC CIs, any threat affecting few critical locations in JIC could result in a major interruption/disruption of the provided services leading to an adverse economic impact at the global level.

3. The open nature and ease of access to JIC CIs make them easy potential targets for terrorist threats. These threats may be imminent or with very short prior warnings.
4. The Saudi Government, through its affiliated Security Forces highly values the protection of human lives that may be lost as a result of attacks on the CIs that are adjacent to densely populated areas.
5. Incident response and security actions should be observed during incident response and crisis management times.
6. Many private and government entities' expertise will effectively combat terrorism and will respond jointly to occurring incidents.
7. Because of the multitude of the JIC stake holders, different security measures and responses are expected. Therefore, the protection of the critical locations, as proposed by our study, should be tightly coordinated between the concerned entities.

## **1.5 Research Contributions**

Most of the CIs are potential targets and protecting all their components seems to be impossible. It is impractical to protect every component of all sectors due to their complexity or the latter ones and their interdependencies. Previous reports such as the one issued by the National Research Council [11] offer a large number of

recommendations to protect these CIs. But implementing all of them would be costly and ineffective.

The petrochemical industry represents the Achilles' heel of the national economy and welfare. There are many aspects to be considered in modeling the CI interdependencies. A systematic approach that identifies the significant relevant risks is needed to protect CIs from terrorist threats and attacks. Due to the complexity and widespread nature of the CIs, their protection is a major technical challenge. There are many practical and theoretical challenges to the development of effective methods that are capable of modeling and planning for CI threats and coordinating actual and decisive responses to combat them.

Furthermore, in this Thesis, we aim to propose efficient mechanisms to “optimally” allocate limited resources to reduce the overall risk threatening the safety of the CIs. The deployment of these limited resources is usually quantified through financial cost estimation. Therefore, a screening methodology is needed to determine the cost distribution of the available resources. The sought screening methodology is expected to combine key asset identification with a quantitative analysis to guide the decision makers in their cost allocation the protection of the most critical components of the CIs.

Furthermore, this Thesis discusses a methodology for identifying the critical locations in the petrochemical industry. A critical location can be defined as a point where a successful attack could lead to devastating consequences. Some critical locations may be easily identified but other locations may only be revealed through an analysis of the

CIs. This methodology can identify individual critical locations and their combinations, which could lead to significant consequences when attacked through simultaneous or sequential events. All the critical locations will be ranked according to their potential impact which will be used as the basis of risk informed decision making.

## **1.6 Structure of this Thesis**

This thesis is outlined as follows. In Chapter 2, an introduction to CIP and its relation to network theory are presented. Also, several CI interdependency models are addressed in this chapter. Next, in Chapter 3, risk analysis model are described. Then, a proposed methodology based on this model to protect CIs at JIC is presented. Some background material on the petrochemical industry at JIC is given in chapter 4. The petrochemical industry at JIC is taken as a case study for the proposed model. Six scenarios are studied including both machine failure and terrorist attack. The conclusions are summarized in Chapter 5, which also includes suggestions for future research.

## **Chapter Two: Literature Review**

### **2.1 Introduction**

The petrochemical industry uses oil and natural gas as major raw materials to produce petrochemical products. Oil and natural gas are composed primarily of hydrocarbons. Most petrochemicals contain hydrogen or carbon or both. Petrochemicals can be converted into thousands of industrial and consumer products, including plastics, paints, rubber, fertilizers, detergents, dyes, textiles and solvents. The industry consists of primary and secondary divisions. The former produces basic petrochemicals, such as ethylene, from oil or gas. The latter converts these petrochemicals to materials that may be directly used by other industries [12].

Most of the Gulf Countries Council (GCC) countries have already in place a healthy and growing base in chemical production that utilizes methane, ethane and gas liquid feedstock in petrochemical units. From 2000 to 2006, the average of GCC investment value growth in chemicals and petrochemicals was 5% [13]. Also, workforce in this sector reached 163,134 workers in 2006 [13]. By the year 2020, investments in this sector are expected to exceed US \$120 billion. The petrochemical sector is an important growth component of the GCC overall industrial sector [11].

The annual business for the U.S. chemical industry is about US \$664 billion. It directly employs more than 800,000 workers and indirectly about 4,790,000 workers. American Chemistry Council (ACC) members have invested nearly US \$6 billion to further enhance

security at chemical facilities over the last six years [14]. From a security perspective, chemical facilities could be converted into weapons of mass destruction. About 600 facilities could each potentially threaten between 100,000 and a million people and about 2,300 facilities could each potentially threaten between 10,000 and 100,000 people within “vulnerable zones” at these facilities [15].

Also, an attack on a petrochemical facility could disrupt economy or impact other CIs. The chemical manufacturing industry supplies other industries with key products (agriculture, pharmaceuticals, drinking water and food processing) [16]. In general, a failure in CI will have a significant impact on other sectors to perform necessary functions.

The majority of experts in the petrochemical industry agree that the chemical facilities are attractive targets for terrorists [16]. Also, they believe that current security conditions at most petrochemical facilities are insufficient [17].

There are several approaches to provide additional security to CIs. The first approach argues that the private sector should shoulder the majority of responsibility for providing additional security measures to petrochemical facilities. It is believed that market forces are sufficient to protect petrochemical facilities from terrorist attacks without any external interference. According to the 9/11 Commission Report, the private sector controls 85% of the petrochemical facilities [17]. In addition, the American Chemistry Council (ACC) says more actions are forthcoming and that the trade

association will continue to prevent chemical facilities and their products from being used to harm anyone [18].

On the other hand, there are those who believe that the private sector and the current requirements alone are not sufficient to improve the protection of the petrochemical facilities from terrorism. The second approach relies heavily on mandates to force plant officials to provide tasks' list for their site protection. They believe that without mandates, any added protective measures by the industry will likely be ineffective [19], [20].

Standing between the two views, there are those who believe that none of these approaches will effectively solve the problem. They argue that there is an urging need for the creation of partnerships between the private and public sectors and those they should work collaboratively with the national security to reduce the attractiveness of petrochemical facilities as targets of terrorism. This cooperative solution will yield more comprehensive and effective long-term results [21].

## **2.2 The Relationship between Network Theory and CIP**

According to Lewis (2006), CIs sectors are naturally modeled as networks where assets are the nodes and the relationships between pairs of assets are links. In this way CIs can be understood, analyzed and then protected using Network Theory [6]. Using network theory, CIs can be modeled as graphs containing nodes, links and a map that tells which nodes are connected to other nodes in the network. Also, it can be used practically to model, analyze and harden potential targets in every CI sector. Like power grid, gas,



water supply system and petrochemical industries, CIs can be modeled as networks and analyzed to identify assets that may be at risk. Based on this, network theory, an area of applied mathematics and part of graph theory, is applied as a framework to analyze CIs because a network clearly identifies the structures of these CIs. For example, petrochemical industry can be modeled as a network of plants (nodes) and pipes (links). Applying network theory to CIs allows using several analysis techniques to the modeled network to know more about the modeled CI. In this case, several issues could be addressed such as “are these two plants connected by critical pipes?”, “does the overall production network have single points of failure?” and “are connections between plants responsible for the cascading failures?” [6].

Networks can be defined as a collection of nodes and links that connect pairs of nodes [6]. Modeling CIs as networks have been discussed in several publications like [22], [23]. More formally, the study of networks is based on graph theory because networks are mathematical graphs [6]. A graph  $G$  is an ordered triplet  $(V(G), E(G), \Psi)$  and  $G$ . It consists of a nonempty set  $V(G)$  of vertices, a set  $E(G)$  of edges and an incidence function  $\Psi_G$  that associates with each edge of  $G$  an unordered pair of vertices of  $G$ . If  $e$  is an edge and  $u$  and  $v$  are vertices such that  $\Psi_G(e) = (u, v)$ , then  $e$  is said to join  $u$  and  $v$  [24]. For example, let  $G = (V(G), E(G), \Psi_G)$  where

$$V(G) = \{v1, v2, v3, v4, v5, v6\} \quad (1)$$

$$E(G) = \{e1, e2, e3, e4, e5, e6\} \quad (2)$$

$$\Psi G(e1) = (v1, v2)$$

$$\Psi G(e2) = (v2, v3)$$

$$\Psi G(e3) = (v3, v4)$$

$$\Psi G(e4) = (v3, v5)$$

$$\Psi G(e5) = (v3, v6)$$

$$\Psi G(e6) = (v5, v6)$$

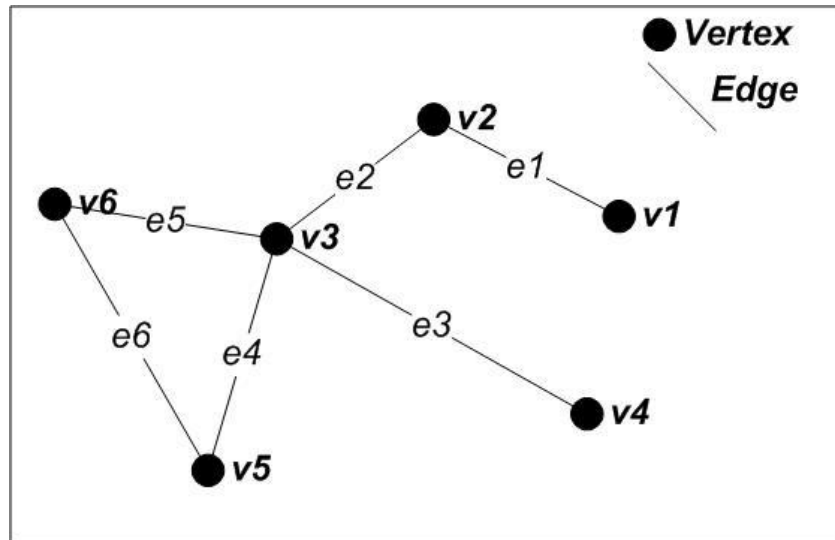


Figure 2-1 Diagram of graph G

For any graph  $G$ , with  $v$  vertices and  $e$  edges, there is a corresponding  $(v \times e)$  matrix which is called the incidence matrix of  $G$  [25]. The incidence matrix  $M(G) = [m_{ij}]$ , where

- $m_{ij} = 0$ , if vertex  $i$  and the edge  $j$  are not incident;
- $m_{ij} = 1$ , if edge  $j$  either begins or ends at the vertex; and
- $m_{ij} = 2$ , if edge  $j$  both begins and ends at the vertex  $i$ , making edge  $j$  a loop.

The incidence matrix is created to serve as the input table for computer analysis. In this thesis Mathematica software is used as a graph analysis tool. Table 2-1 shows the incidence matrix  $M(G)$  for the graph  $G$  shown in Figure 2-1.

		Edges					
		e1	e2	e3	e4	e5	e6
Vertices	v1	1	0	0	0	0	0
	v2	1	1	0	0	0	0
	v3	0	1	1	1	1	0
	v4	0	0	1	0	0	0
	v5	0	0	0	1	0	1
	v6	0	0	0	0	1	1

Table 2-1 Incidence matrix for graph G

If there is a path between two vertices  $u$  and  $v$ , then they are “connected”. For example, in graph G vertices  $v1$  and  $v5$  are connected along path  $v1, e1, v2, e2, v3, e4$  and  $v5$ . An edge/vertex is called “a cut edge/vertex, if its removal from the graph results in separating the graph into two distinct sections. For example the cut edges for graph G are:  $e1, e2$  and  $e3$  and the cut vertices are:  $v1, v2, v3$  and  $v4$ . A cut set  $S$  is a set of components (edges and vertices) which, if removed from the graph, would result in separating the graph into two distinct sections [25]. A cut set is called minimal (MCS) if it cannot be reduced without losing its status as a cut set [25].

According to [25], a directed graph  $D$ , also called a digraph, is an ordered triplet  $(V(D), A(D), \Psi_D)$ . It consists of a nonempty set  $V(D)$  of vertices, a set  $A(D)$  of arcs and an incidence function  $\Psi_D$  that associates with each arc of  $D$  and ordered pair of vertices of  $D$ . If  $a$  is an arc and  $u$  and  $v$  are vertices such that  $\Psi_D(a) = (u, v)$  then  $a$  is said to join  $u$  and  $v$  where  $u$  is the tail of  $a$  and  $v$  is its head. Arc  $a$  allows flow from  $u$  to  $v$ , but not from  $v$  to  $u$ . For example, let  $D = (V(D), A(D), \Psi_D)$ , where

$$V(D) = \{v1, v2, v3, v4, v5, v6\} \quad (3)$$

$$A(D) = \{a1, a2, a3, a4, a5, a6\} \quad (4)$$

$$\Psi_D(a_1) = (v_1, v_2)$$

$$\Psi_D(a_2) = (v_2, v_3)$$

$$\Psi_D(a_3) = (v_3, v_4)$$

$$\Psi_D(a_4) = (v_3, v_5)$$

$$\Psi_D(a_5) = (v_3, v_6)$$

$$\Psi_D(a_6) = (v_6, v_5)$$

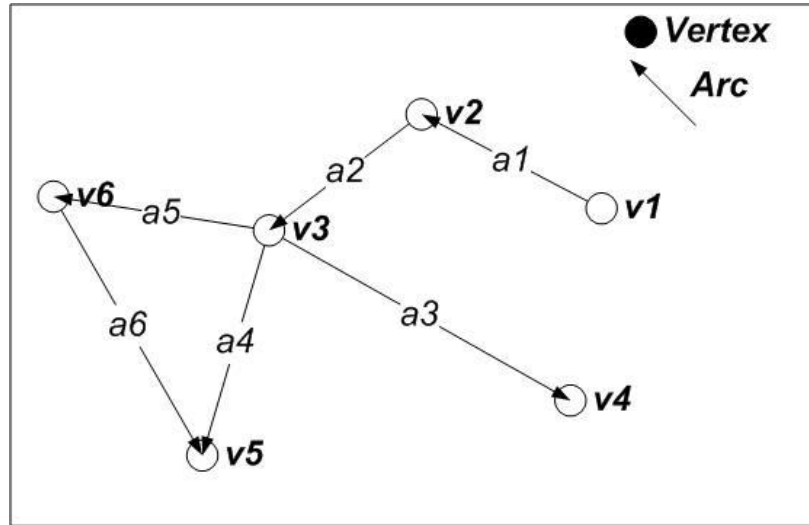


Figure 2-2 Digram of digraph D

Similar to graphs, digraphs have also an incidence matrix. The incidence matrix  $N(H) = [n_{ij}]$ ,

where:

- $n_{ij} = 0$ , if the vertex  $i$  and the arc  $j$  are not incident;
- $n_{ij} = 1$ , if the head of arc  $j$  is incident with vertex  $i$ ;
- $n_{ij} = -1$ , if the tail of arc  $j$  is incident with vertex  $i$ ; and
- $n_{ij} = 2$ , if arc  $j$  both begins (tail) and ends (head) at the vertex  $i$ , making arc  $j$  a loop.

Table 2-1 shows the incidence matrix  $N(D)$  of the digraph D.

		Arcs					
		$a_1$	$a_2$	$a_3$	$a_4$	$a_5$	$a_6$
Vertices	v1	-1	0	0	0	0	0
	v2	1	-1	0	0	0	0
	v3	0	1	-1	-1	-1	0
	v4	0	0	1	0	0	0
	v5	0	0	0	1	0	1
	v6	0	0	0	0	1	-1

Table 2-2 Incidence matrix  $N(D)$  for digraph D

Two nodes  $u$  and  $v$  are connected if a direct path exists from  $u$  and  $v$ . In digraph  $D$ , vertex  $v1$  is connected to vertex  $v5$  along the directed path  $v1, a1, v2, a2, v3, a4$  and  $v5$ . But, vertex  $v5$  is not connected to vertex  $v1$  because there is not a directed path from vertex  $v5$  to vertex  $v1$ . The concept of a cut set on graph is the same for digraphs.

In this thesis, CIs are modeled as a digraph, Vertices represent the plants and arcs represent the pipes that connect the plants. In this case, we are interested in identifying the events that interrupt the production of these plants. Let the digraph  $D$  represent the petrochemical industry at JIC as shown in Figure 2-3. 14 vertices (nodes) represent the JIC's plants and 36 arcs represent pipes the connecting these nodes. Table 2-3 shows the Incidence matrix of petrochemical industry network at JIC . All the nodes are connected to each other via pipes to get their raw material needed for their production. This means that some nodes produce some raw material for other nodes (consumers). To avoid any disruption in the petrochemical industries at JIC, the cut sets (cut arcs and vertices) responsible for such failures must be identified. Although the petrochemical industry network is modeled as the digraph shown in Figure 2-3, minimum cut set (MCS) technique is not applicable in this situation. We found that heterogeneous networks, such as petrochemical networks of interest to this thesis, cannot be analyzed as regular digraph. Therefore, a major contribution of this thesis is the development of a MCS technique to handle heterogeneous networks.

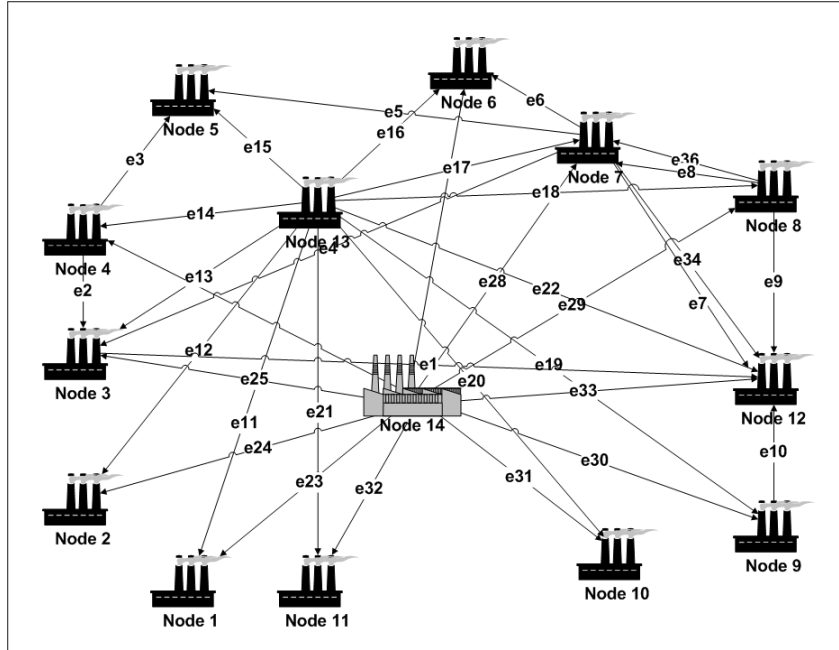


Figure 2-3 Diagram for digraph of petrochemical network at JIC

In regular digraphs, all the links carry the same raw material e.g. water is carried in pipes in all water supply networks, signals are transmitted in all computer networks and power is flown over the entire power grid network. However in petrochemical networks each link is carrying different material. For example, if MCS technique is applied to node1 in Figure 2-3 the MCS sets will be  $\{e23, e24\}$  which is not true. Node1 requires both gas (e24) and petrol (e23) to work in a proper way. Therefore the MCS set for node1 is given by  $\{e23\}, \{e24\}$ .

To solve this issue, we propose, in this thesis, a new MCS technique to find the MCS in all heterogeneous networks. This technique is called PMCS (Production Minimal Cut Set) which will be covered in the next Chapter. In analyzing CI networks (digraphs) for all

nodes, one is interested to find all the cut sets which have the greatest impact on the network when it is successfully attacked.

	e1	e2	e3	e4	e5	e6	e7	e8	e9	e10	e11	e12	e13	e14	e15	e16	e17	e18	e19	e20	e21	e22	e23	e24	e25	e26	e27	e28	e29	e30	e31	e32	e33	e34	e35	e36
Node 1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Node 2	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Node 3	-1	1	-1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Node 4	0	-1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Node 5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Node 6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Node 7	0	0	0	-1	-1	-1	-1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	-1	-1	1
Node 8	0	0	0	0	0	0	0	-1	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	-1
Node 9	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Node 10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Node 11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Node 12	1	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0
Node 13	0	0	0	0	0	0	0	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Node 14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	0

Table 2-3 Incidence matrix of petrochemical industry network at JIC.

## 2.3 CI Characteristics

Lewis summarizes the major characteristics of CIs as follows [6]:

- **Vastness:** Each sector in the CI is a vast network. It is so large and complex network that it is impractical to protect every component of each sector. It is wide because it covers a large geographical area. It has also many components or it is complex. For example, in the water sector in the U.S., there is the Colorado River Basin, which provides hydroelectric power and irrigation for 25 million people. It spans 250,000 square miles and is shared by seven states and local governmental entities, including Mexico and the water rights owned by the Native Americans. If protecting a single CI is a daunting task, protecting all the CI components of all sectors seems to be impractical if not impossible.
- **Command:** The interdependency of government agencies, public and private sectors, as well as the regulatory and economic drivers makes the problem of “who is in charge” a major barrier to CIP. There is no central point of control in most of the CI. For several reasons, most of the CIs are beyond the reach of direct governmental control.
- **Information Sharing:** The lack of information sharing causes inefficiencies and vulnerabilities in the CIP exercise. CIs are under the control of several companies. There is a major challenge in simply collecting and correlating information. There are technical and organizational reasons that make information sharing difficult.



Most of the time, these systems are incompatible or hold their information in databases that have different indexes, formats and encodings. This would lead to interoperability problems. Interoperability of information systems is a major limiting factor preventing information sharing. Most of the information needed to effectively prevent attacks on CIs is highly sensitive. Legal, cultural and bureaucratic sensitivity runs high among agencies that need to share information.

- **Knowledge:** The technology behind various CIs is vast and complex and yet it is necessary to understand these underlying technologies before effective strategies and policies can be enacted. At this stage, there is insufficient information about CIP. The technology of CIP begins with an understanding of the technology of individual sectors. This requires an understanding of electrical power generation and transmission, the technology of telecommunications, the protocols of the Internet, the science/engineering of petrochemicals, etc. The inner workings of the intermodal transportation system, banking and finance, water and utilities, gas and oil pipelines and so on must be understood before strategies and policies can be made. Therefore, comprehension of technologies is a prerequisite for making an effective strategy for the protection of the nation's CIs.
- **Inadequate Tools:** The study of the vulnerability of CIs is a new area of research and, as such, the information about CIs needed to propose general approaches

or general solutions is rather scarce. Tools and techniques are needed for modeling complex CIs, understanding their interdependencies, analyzing their vulnerabilities and finding optimal means of protection. Almost every aspect of CIP is lacking in terms of a foundational theory and applied proven tools.

- **Asymmetric Conflict:** CIs are particularly vulnerable to asymmetric attacks. Asymmetric attacks look for high payoff targets that can be damaged by a small force. CI vulnerabilities provide an opportunity for attackers to magnify their firepower through asymmetric techniques. CI is an easy target for the attacker because most sectors are relatively exposed, vast and with little protection. An Internet search engine such as Google can be used by anyone to discover the locations of critical components. Also, small forces can make a major impact because the most valuable assets of most sectors are concentrated in a small number of critical components or locations. Significant attacks can be mounted with little force because they require knowledge more than they do forces. For example, most telecommunications assets are housed in a relatively small number of buildings. These components can be attacked by a single person.
- **Interdependencies:** CI sectors are complex because of their interdependencies. Interdependencies are due to human organizational structures as well as technical\physical linkages between components of a single sector and those of other sectors.

Interdependencies within a sector and across multiple sectors complicate the problem of inadequate sector-specific knowledge. For example, the power grid is so complex that the simplest failure in a single power line can propagate like a contagion through a crowded population area [6]. Such scenario occurred in the 2003 blackout [6]. Besides the inherent complexity of such sophisticated CIs, every CI sector is connected to, and hence interacts with, almost all other CI sectors.

## **2.4 Dependency**

Dependency can be defined as a connection between two CIs through which the state of one CI influences or is correlated to the state of the other one [26]. Consider an individual connection between two CIs such as the electricity (i) used to power a telecommunications (j) switch. In this case, the relationship is usually unidirectional; CI (j) depends on (i) through the link, but (i) does not depend on (j) through the same link. Figure 2-4 illustrates the electric power infrastructure dependencies [26].

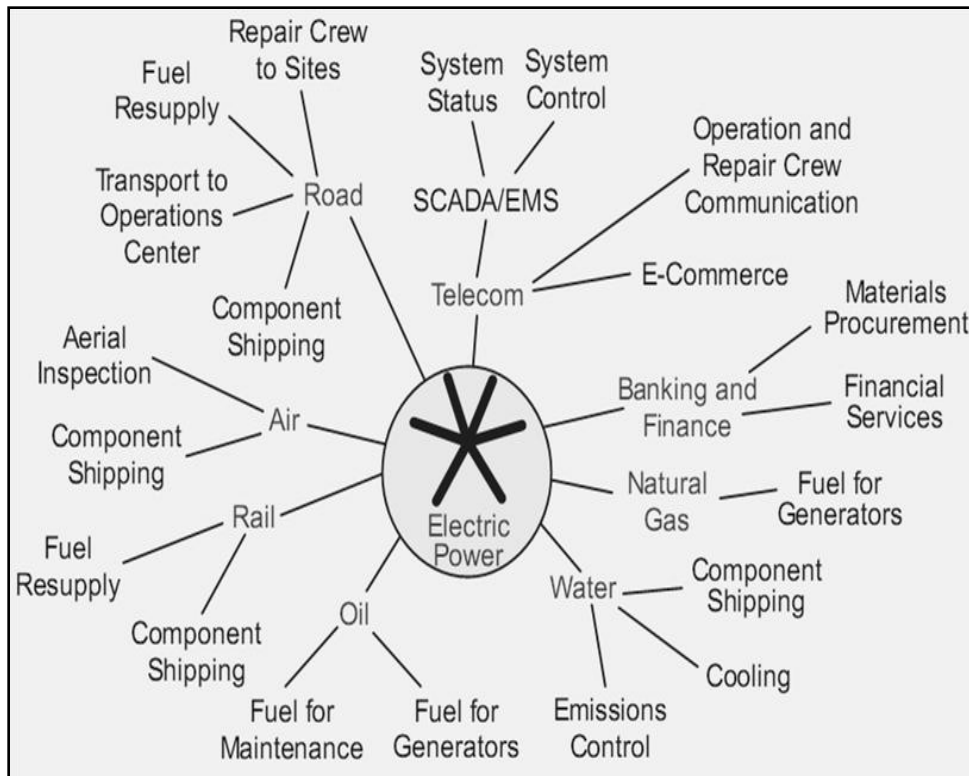


Figure 2-4 Examples of electric power infrastructure dependencies [26].

Electric power infrastructure needs natural gas and petroleum fuels for its generators, road and transportation to supply fuel to the generators, water for cooling, banking and finance for fuel purchases and telecommunications for monitoring system status and system control (i.e., supervisory control and data acquisition (SCADA) systems and energy management systems (EMSs)) [26]. During emergencies or after component failures, the electric power infrastructure will have potentially different critical dependencies on the same infrastructures. For example, the utility may require petroleum fuel for its emergency vehicles and emergency generators and road transportation to dispatch repair crews and spare components. As depicted in Figure 2-

4, electric power is the supported CI and natural gas, oil, transportation, telecommunications, water and banking and finance are supporting CIs [26].

## 2.5 Interdependency

Interdependency is a bidirectional relationship between two CIs where the state of each CI influences the state of the other [26]. Usually, CIs are connected at multiple points through a wide variety of mechanisms such that a bidirectional relationship exists between the states of any given pair of CIs; infrastructure (i) depends on (j) through some links, and (j) likewise depends on (i) through other links. More generally, two CIs are interdependent when each one is dependent on the other. The term interdependency means that the connections are established among agents in different CIs in a general system of systems [26].

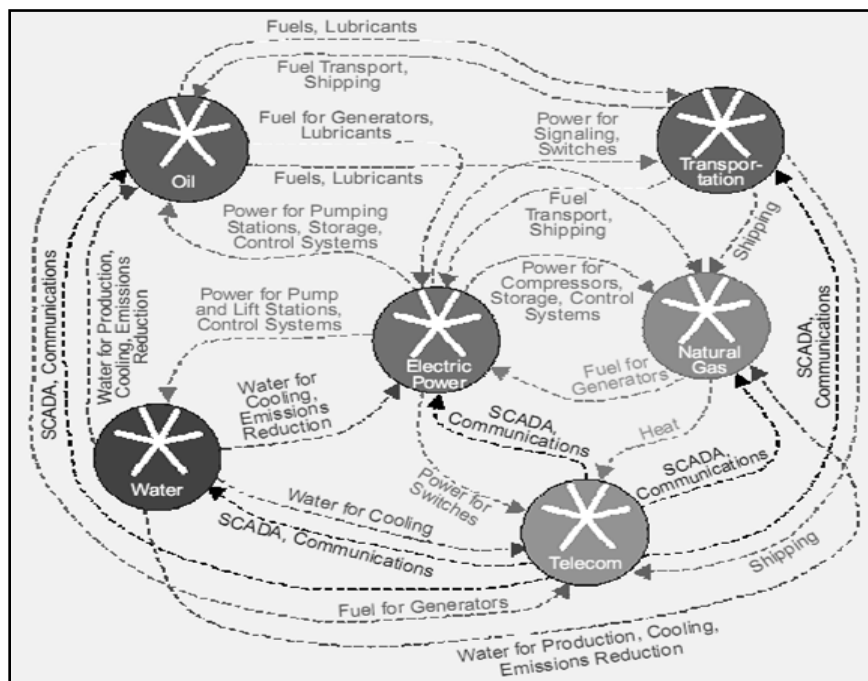


Figure 2-5 Example of CI interdependencies [26].

The interdependent relationship among several CIs is shown in Figure 2-5 [26]. These complex relationships are characterized by multiple connections among CIs, feedback and feed forward paths, and intricate, branching topologies. It is clearly impossible to understand the behavior of a given CI in isolation from other CIs [26].

There are four types of interdependences: 1) physical interdependency; 2) Cyber Interdependency; 3) geographic interdependency; and 4) logical interdependency.

### **2.5.1 Physical Interdependency**

Physical interdependency occurs when the state of a CI is dependent on the material outputs of another CI [26]. It means that the physical output of one CI is the physical input to another CI [27]. For example, a rail network and a coal fired electrical generation plant are physically interdependent, given that each supplies commodities that the other requires to function properly [26]. The railroad provides coal for fuel and delivers large repair and replacement parts to the electrical generator, while electricity generated by the plant powers the signals, switches and control centers of the railroad. The state of one CI directly influences the state of the other and vice versa. The state change in the railroad can drive a corresponding state change in the electrical grid. Consequently, the risk of failure in one CI can be a function of risk in a second CI if the two are interdependent.

### **2.5.2 Cyber Interdependency**

Cyber interdependency occurs when the state of a CI depends on information transmitted from another CI [26]. Cyber interdependencies are relatively new and are a

result of advanced computerization and networking [27]. Disruptions in one CI may or may not cause disruptions in another CI, depending on the nature and magnitude of the disruption. The CIs are connected to each other via electronic and informational links. The information output of one CI is the information input to the other CI.

### **2.5.3 Geographic Interdependency**

Geographical interdependency occurs when CIs are located in one area and an environmental event can create state changes in all of them [26]. For example, fire could create correlated changes in the geographically interdependent CIs. An electrical line and a fiber-optic communications cable slung under a bridge connect (geographically) connect elements of the electric power, telecommunications and transportation infrastructures. Due to proximity, they are geographically interdependent. Traffic across the bridge does not affect the cables but physical damage to the bridge could affect the electric power, communications and transportation infrastructures [26].

### **2.5.4 Logical Interdependency**

Logical interdependency occurs when the state of two CIs depends on the state of the other via a mechanism that is not a physical, cyber or geographic connection [26]. It means that the state of one CI depends on the state of another CI. It is usually via human decisions and actions. For example, a lower gas price increases the flow of gasoline and traffic congestion. In this case, the logical interdependency between the

petroleum and transportation infrastructures is due to human decisions and actions [27].

## **2.6 CIP Case Studies**

### **2.6.1 USA**

According to [28], nearly five million Americans live within a five mile radius of the most hazardous chemical facilities in the U.S. Before the 9/11 events, there was no single agency in the government whose core mission is to protect against and respond to an attack on one of these major facilities. There were twelve different government entities supervising the protection of USA's CIs [28]. After 9/11, the Department of Homeland Security (DHS) was established [29]. CIP efforts were merged within the new Department as well as the twenty two relevant federal agencies transferred to the DHS including the following [29]:

- The National Infrastructure Protection Center (NIPC) which is an expansion of the FBI's Computer Crime Division into a focal point for national threat assessments, vulnerability analysis, investigations and response coordination in the information systems and computing sectors.
- CI Assurance Office (CIAO) which support individual agencies developing plans, helps coordinate national education and awareness campaigns and provides legislative and public affairs support.
- The National Infrastructure Simulation and Analysis Center (NISAC) which is a modeling, simulation and analysis program that prepares and shares analyses of



the CIs and the key resources including their interdependencies, vulnerabilities, consequences of disruption and other complexities.

- Information Sharing Analysis Centers (ISACs) which gathers and analyzes information on threats and incidents and shares this information with Government entities.

The US DHS Department builds and maintains a comprehensive assessment of the infrastructure sectors: food, water, agriculture, health systems and emergency services, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail and ports), information and telecommunications, banking and finance, energy, transportation, chemical, defense industry, postal and shipping and national monuments and icons. The Department develops and harnesses the best modeling, simulation and analytic tools to prioritize effort, taking as its foundation the National Infrastructure Simulation and Analysis Center (currently part of the Department of Energy) [28].

DHS relies on a cooperative approach between government agencies and the private sector to determine and address vulnerabilities [30]. The American CIP system is relatively transparent [31].

### **2.6.2 Canada**

The Government of Canada is working cooperatively with provinces, the private sector and the international community to protect CIs. The Federal Government brings greater accountability to the CIP at the Federal level. The Minister of Public Safety has introduced the Emergency Management Act (EMA), which modernizes the

Government's approach to emergency management and aligns federal roles and responsibilities with today's realities and threat environment [32]. As part of the EMA, federal ministers are responsible for identifying risks to CI within their respective areas. Also, each department is required to develop emergency plans to address these risks. Each department maintains tests and exercises these emergency management plans according to the policies and programs established by the Minister of Public Safety.

Canadians want all levels of government working together to protect their CIs. Canada's national approach has two parts; first, the National Strategy for CIP which clarifies all the concepts relevant to all CI sectors and their challenges [32]. Moving forward with this collective approach, the National Strategy will serve as the basis for enhanced collaboration between all levels of Government and the private sector.

The second element of Canada's national approach is the development of a flexible Action Plan (AP) that builds on the National Strategy. It will be updated on an iterative basis to enable partners to anticipate new risks and adopt new best practices [3].

The National Strategy for CIP and the supporting AP, in addition to the Emergency Management Act, establish a collective approach that can be used to set national priorities, goals and requirements for CIP. This collective approach will enable funding and resources to be applied in the most effective manner to reduce vulnerabilities, mitigate threats and minimize the consequences of attack and disruptions [32].

On March 1, 2004, Public Safety and Emergency Preparedness Canada (PSEPC) and the Science and Engineering Research Canada (NSERC) start a new academic research program to investigate infrastructure interdependencies. The Joint Infrastructure Interdependencies Research Program (JIIRP) is part of the national efforts to secure and protect Canada's CIs [33].

JIIRP produces new science-based knowledge and practices to better assess, manage and mitigate risks to Canada from failures in its CIs. This program is designed to help infrastructure owners and operators better understand the extent of their dependencies on other sectors for delivering their services and goods. It also provides process that mitigates the risk resulting from these interdependencies. The goal of the JIIRP is to bring together all organizations, with a stake in safeguarding CIs, to develop partnerships and methods of information exchange [33].

Also, the JIIRP program aims to expand academic, industrial and government research activities in the area of infrastructure interdependencies; to develop relevant new knowledge, techniques and policies. It aims also to raise awareness of infrastructure interdependency and build partnerships across Canada and among relevant disciplines to facilitate effective transfer and dissemination of research results to the private and public sectors [33].

### **2.6.3 The United Kingdom**

Although CIP started to be a concern at the highest level at the end of 1990s, the bomb attacks in London in July 2005 were a reminder that the threat from terrorism is real

and serious. In February 1st, 2007, the Center of Protection of National Infrastructure (CPNI) was formed from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC). NISCC provided advice and information on computer network defense and other information assurance issues. NSAC provides also advice on physical security and personnel security issues. However, CPNI provides integrated security advice to the businesses and organizations which make up CIs. Through the delivery of this advice, UK protects national security by helping to reduce the vulnerability of CIs to terrorism and other threats [34].

#### **2.6.4 Australia**

The Australian model is based on consultation and cooperation between the owners and operators of CIs and governments. CIP requires the active participation of the owners and operators of CIs, regulators, professional bodies and industry associations, in cooperation with all levels of government and the public. In April 2003, The Trusted Information Sharing Network (TISN) was established [35]. TISN is a forum in which the owners and operators of CIs can work together by sharing information on security issues which affect their CIs. The network is made up of a number of Infrastructure Assurance Advisory Groups (IAAGs) for different business sectors and is overseen by the CI Advisory Council (CIAC) [36].

The Australian Government's CIP Modeling and Analysis Program (CIPMA) aims to enhance the protection of Australia's CI and improve the resilience of the economy

and society [35]. CIPMA shows how different parts of Australia's CI rely on each other. It also shows in detail what would be the consequences if a CI fails. CIPMA is an invaluable aid for decision makers to protect CIP and to counter terrorism.

#### **2.6.5 Germany**

The CIP (CIP) Working Party of Federal Ministries was set up in Germany in 1997. It works under the leadership of the Federal Ministry of the Interior (BMI). Many campaigns, such as Security on the Internet and the setting up of special commissions are intended to increase awareness of the protection of CIs [31].

The Federal Office for Information Security (BSI) works as a coordination function and makes security technologies and solutions available [37]. The German system for the protection of CIs is not very transparent to outsiders. Since 9/11 events, the work in the area of protection of CIs has been growing noticeably. The CI studies carried out by the BSI in 2002 make Germany one of the few countries that are following an analytic and process-oriented approach [37].

### **2.7 CI Interdependencies Modeling**

The study and analysis of the interdependencies between CIs is relatively new. The increase of funding and level of efforts has led to much innovative work in this area. Therefore, while modeling of CI interdependencies has begun recently, many modeling approaches have been implemented to model interdependent CIs. Each of these models has its own strengths and weaknesses. In this Chapter a review of several approaches is given.

### **2.7.1 A Screening Methodology for the Identification and Ranking of CIs**

#### **Vulnerabilities due to Terrorism**

Apostolakis and his group at MIT started in 2005 to build a screening methodology for the identification and ranking of CIs. Apostolakis and Lemon [10] propose a methodology for identifying and prioritizing the vulnerability in CIs. They modeled CIs as digraphs and used graph theory to identify vulnerable scenarios which are screened for susceptibility to terrorist attacks. Also, all CIs' elements are prioritized according to their vulnerabilities using multi-attribute utility theory (MAUT). Then, a value tree, built based on perceptions of the decision-makers, is used to show the impact of losing CI services. This method was applied at MIT. Three interconnected CIs, (natural gas, water and electricity) were analyzed. It is worth nothing that our methodology, proposed in this thesis, applied to both homogeneous and heterogeneous CI networks.

Michaud and Apostolakis [38] proposed a scenario-based methodology for the ranking of the elements of a water-supply network based on feedback from the decision maker. This methodology is based on MAUT and a graph theory. They extended the approaches proposed by Apostolakis and Lemon [10] by taking into consideration the capacity of the CI's elements and their mean time to repair. This model is applied to water supply infrastructure in a midsize city. The water supply infrastructure is modeled as a network. Then, scenarios were created to evaluate the result of the failure of each of its elements. For each scenario, the supply level to the various users considering the capacity of their connection to the available resources is evaluated. Using MAUT the disutility of this supply level is evaluated and provided to the decision makers. Two

types of failures (random causes and malevolent failures) were considered. Random failures which are ranked according to their expected disutility and malevolent acts failures are ranked using a subjective combination of the disutilities and the scenario susceptibility to attack. The results are provided to the decision makers for evaluation and risk management.

Apostolakis and Patterson [39] presented an approach for ranking geographic regions that can affect multiple CIs. This approach shows how the methodology can bring attention to areas that are important when several infrastructures are considered. It identifies the critical locations by calculating a value for a geographic region that represents the combined values to the decision makers of all CIs. A performance index (PI) to each CI using MAUT based on their disutility of the loss. Then, importance measures (IM) are given to all the elements of each CI using Monte Carlo network analysis. IMs and PIs are combined into one value which represents a value worth (VW) for each infrastructure's elements independently. Then, a spatial analysis technique within a geographic information system (GIS) is used to combine the VWs of each infrastructure elements in a geographic area into a total value called geographic valued worth (GVW). All GVW values are displayed in the GIS system in a color scheme. Using this map, decision makers can determine whether these regions are critical locations to allocate anti-terrorism resources to. This model was successfully applied at MIT.

Apostolakis et al. [40] proposed a methodology to perform a risk analysis on the bulk power system. This method is performed for failures of CI elements due to both random

causes and malevolent acts. A power flow simulation mode is used to determine the likelihood and extent of power outages when components within the system have failures. The result of these failures is determined by looking at the type and number of customers affected. Then, the decision makers evaluate the importance of these consequences and rank each system component by its risk significance.

Apostolakis et al. [41] developed a systematic methodology that combines Probabilistic Risk Assessment (PRA), decision analysis and expert judgment to assess and rank the risks from multiple hazards. Scenarios were used to show how initiating events result in undesirable consequences. MAUT technique is used to build a value tree. The latter is based on the decision-makers preferences about the impacts on CIs and other assets. The performance index (PI) enables the ranking of the risks from random failures and malicious acts. The MIT Campus was considered for a case study of a real project.

### **2.7.2 Inoperability Input-Output Model for Interdependent Infrastructure**

Haimes and Jiang proposed [42] and presented a Leontief-based infrastructure input-output model to analyze the interdependencies and interconnectedness among CIs. This analysis is based on the well known Leontief input-output mode (IOM). The IOM was proposed by Wassily Leontief. Leontief-based infrastructure input-output is intended to be used as a tool to allocate resources for an effective process of risk assessment and risk management. It is considered as a system consisting of  $n$  critical complex and interconnected infrastructures, with the output being their risk of inoperability that can be triggered by one or multiple failures due to complexity, accident, or acts of terrorism.



The input to the system is between 0 and 1 where 0 corresponding to a flawless operable system state and 1 corresponding to the system being completely inoperable.

A holistic risk assessment and management framework for modeling the risks of terrorism to the homeland security were proposed by Haimes [4]. Both the homeland system and the terrorist networks system are addressed here. The centrality of state variables of both systems is modeled. A roadmap for modeling risks of terrorism is also given here.

Haimes et al. [44] developed the Inoperability Input-output Model (IIM), based on Leontief's input-output model, for Interdependent CIs [44]. This model characterized the interdependencies among sectors in the economy and analyzed their relationship to the other sectors. The IIM prioritizes and manages the sectors based on their criticality to the economy. An application of their framework to attacks on electric power and telecommunications is given.

Gerald et al. [45] proposed bi-level models to make CIs more resilient to attacks. These models consist of an intelligent attacker and a defender along with information transparency. These models are Stackelberg games as opposed to two-person or zero-sum games. For example, one model is used to identify locations for a set of electronic sensors that minimize the worst-case time to detection of a chemical, biological, or radiological contaminant introduced into the Washington, D.C. subway system. These models are illustrated with applications to electric power grids, subways, airports and oil pipelines.

### **2.7.3 Agent-Based Model**

In general, the agent-based paradigm has become one of the most popular approaches in the software development. Agent-based models are rule-based simulation models. Agent-based systems provide a way of conceptualizing sophisticated software applications that face problems involving multiple and distributed sources of knowledge. In this way, they can be thought of as computational systems composed of several agents that interact with one another to solve complex tasks beyond the capabilities of an individual agent. The constructed computational agents are used to simulate real phenomena and to provide clues into the natural emergence of behaviors [46]. AIMS, developed by New Brunswick Critical Infrastructures, and CommAspen, developed by Sandia National Laboratories, use such simulations to model CIs as agents to study the interactions between them after some disruptive events [47].

### **2.7.4 Cell-Channel Model**

The cell-channel model is one of the modeling approaches for the CI Interdependencies. It is used in CI Interdependencies Simulator (I2Sim) which was developed at the University of British Columbia [48]. The I2Sim simulate the conditions of each CI component for large disaster scenarios to support decision-making to mitigate the disaster effects. This model is based on the idea of service token delivery to different CI entities. The system consists of cells, channels and tokens. Cells are entities that perform functions. Channels are the means through which tokens flow from one generator node to a load node. Tokens are services that are provided by one entity to another entity that uses them [48], [49].

The cells' functionality is determined by the interrelationship between the input(s) and output(s) and each channel is described using functions with capacity limitations and time delay. The combined cells and channels model makes up the multiple networks system. The cell-channel Model has been used on physical layer modeling of interdependent CIs [49].

#### **2.7.5 Network Models**

A relatively new branch of science has developed in recent years. It describes the interconnectivity between network entities, including social, biological and economic networks [50]. In [51], network model was used to simulate the spreading of disaster in interconnected CIs networks. Also, [52] simulated the effects of node and edge "attacks" on a number of networks using the same model.

## **Chapter Three: Methodology Overview**

### **3.1 Overall Methodology**

Probabilistic Risk Assessment (PRA) was born in the nuclear industry about 30 years ago [53], [54], [55] and has traditionally been focused on complex systems such as nuclear power facilities and space systems. Its primary concept is to identify the most important vulnerabilities by using frequencies and probabilities of component failures. PRA is a systematic process which produces an understanding of the associated risks in engineered systems. This process combines the probability of an event with the anticipated consequences of the event to produce an overall risk of the system. According to [56], PRA asks: what can go wrong? what are the consequences? and how likely is it?

Garrick et al. [57] recommended the PRA framework to identify, quantify and manage terrorist threats. Apostolakis and Lemon [10] proposed the use of PRA to screen terrorism scenarios on CIs. Their methodology, a scenario-based approach, combines Multi-Attribute Utility Theory (MAUT) and PRA. This approach gives each scenario a value that a measure how undesirable is this scenario to the stakeholders. The value is a function of the consequences of a scenario in terms of service interruption. Then the susceptibility of each scenario is measured by calculating the probability of a scenario to become true if a threat materializes. This susceptibility is assessed and combined with the scenario value to produce a vulnerability assessment. A scenario

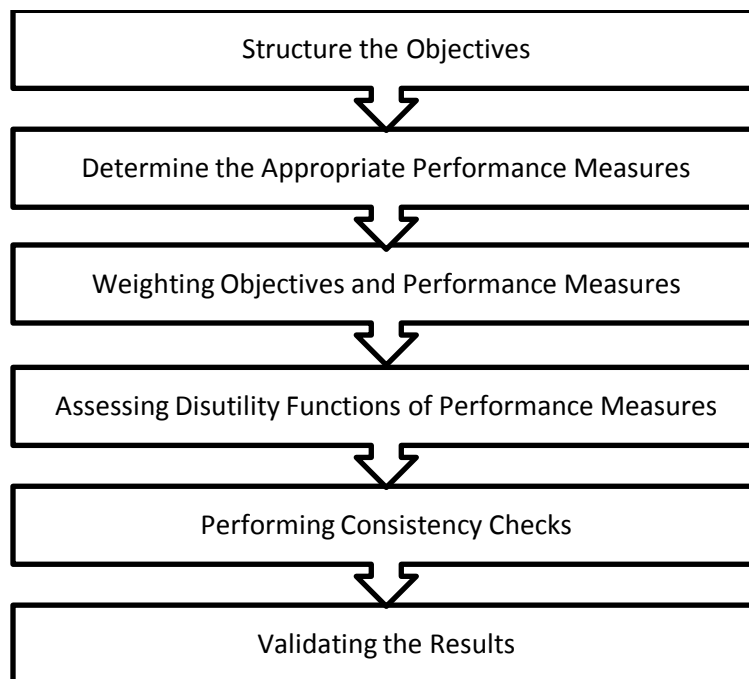
can only represent a critical vulnerability if both its value and its susceptibility are high.

The first step is to identify the assets whose services must be protected. The assets in this thesis will be all the petrochemical plants in JIC. The next step is to identify the scenarios that are initiated by malicious acts, could lead to the interruption of these services. The existing mathematical network analysis [24], [22] is used to model the petrochemical industry CI. The minimal cut sets (MCS) concept [23] is used to identify the sets of events e.g. failures that lead to the interruption of the service. In order to model the petrochemical CI, we let vertices represent the plants and arcs represent the pipes. Then, the MCS (combinations of failures of arcs and vertices) is identified using the network model which interrupts the service to each user. The system will be considered to have failed if the CI service is interrupted. The MCS determines the candidate vulnerabilities of the system. Then, MAUT is used to assign value to each determined vulnerability. The assigned value provides additional information to the decision maker regarding the degree to which a potential target is accessible [10]. A performance index (PI) is calculated for each MCS as shown in Equation (5). The PI index is the sum of the weights of individual performance measures (PMs) multiplied by the disutility of each item for that particular PM. The PMs represent what is important to the decision-maker.

$$PI_j = \sum_i^{K_{pm}} w_i d_{ij}, \quad (5)$$

Where  $PI_j$  is the performance index for MCS  $j$ ,  $w_i$  is the weight of the performance measure  $i$ ,  $d_{ij}$  is the disutility of performance measure  $i$  for MCS  $j$  and  $K_{pm}$  is the number of performance measures. The inequality  $PI_j > PI_m$  means that the decision maker assesses case  $j$  to cause more disutility than case  $m$ .

All MCS are ordered by their PIs which, in turn, indicate which MCS, in the event of a successful attack, would lead to the greatest disutility to the decision-maker and which MCS should be considered as candidate vulnerabilities based on their value to the decision-makers. According to [58], there are six steps to determine the PIs:



Structuring the objectives is necessary to identify the fundamental objectives to the decision maker in analyzing the system. A value tree is used to develop the PMs. The Value tree is a hierarchal approach which represents the fundamental concerns of the

decision-maker [59], [60]. Figure 3-1 shows the proposed value tree for petrochemical industry in JIC.

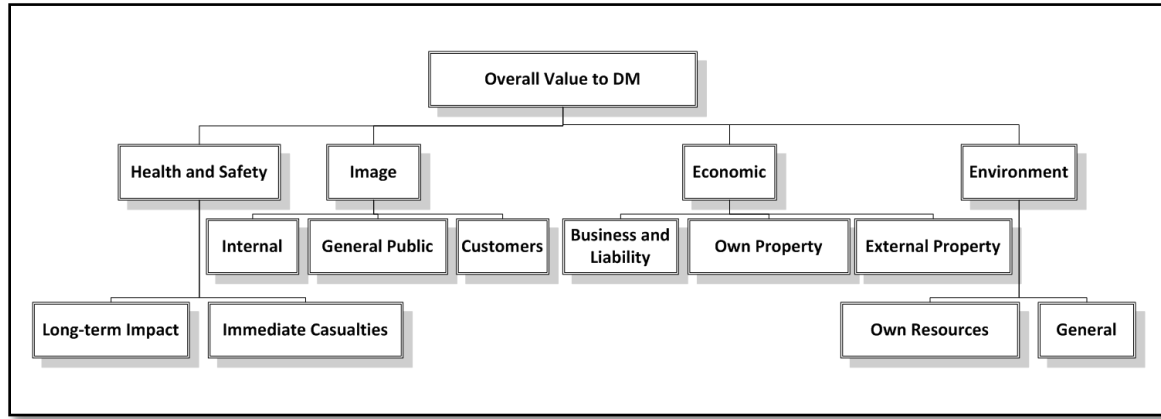


Figure 3-1 Proposed Value Tree for Petrochemical Factories at JIC.

Then performance Measure (PM) is used to measure the magnitude of the impact of each scenario. Impact on health and safety and impact on environment are examples of PM. Natural scales is used to measure the impact level directly, such as dollars for an economic impact, or lost work days for a safety impact. When natural scales do not exist, constructed scales are used. Constructed scales are used to reduce the difficulty of assessment for all the PMs and to allow the decision maker to combine multiple metrics into a single PM [10]. A constructed scale is divided into a sufficient number of zone levels, with a description of the criteria appropriate to that level. Constructed scales will be developed for all the PMs. Table 3-1 shows the constructed scale for physical property damage.

Level	Description
3	Catastrophic physical property damage, Greater than SR 10 million
2	Major physical property damage SR 1 million to SR 10 million
1	Minor physical property damage Less than SR 1 million.
0	No physical property damage

Table 3-1: Preliminary Constructed Scale for Physical Property Damage.

The next step is assigning weights to the objectives and PMs using the Analytic Hierarchy Process (AHP) [61]. It begins with a series of pair-wise comparisons between the fundamental objectives with respect to the primary goal. This comparison is based on a linguistic scale shown in Table 3-2.

Importance Intensity	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective.
3	Weak importance of one over another	Experience and judgment slightly favor one activity over another.
5	Essential or strong importance	Experience and judgment strongly favor one activity over another.
7	Very strong or demonstrated importance	An activity is favored very strongly over another; its dominance demonstrated in practice.
9	Absolute importance	The evidence favoring one activity over another is of the highest possible order of affirmation.
2,4,6,8	Intermediate values	When compromise is needed.

Table 3-2: AHP Comparison Scale [61].

The comparison will be made first for the fundamental objectives. Then, the weight of the fundamental objectives is passed down the value tree to the objectives below. AHP is used to distribute the weights among the objectives [58]. The value tree is completed



when all weights have been passed down the tree to the performance measures. The weights are converted into a 0 to 1 scale using a linear transformation.

After establishing the value tree and weights, the disutility functions are assessed with the associated performance measures. The disutility function is developed by applying AHP to the constructed scale for each performance measure [62]. The pair-wise comparisons of the levels are applied to all PMs. Once the value tree is complete, the preference consistency should be checked for all the PMs. Then, they are converted into a 0 to 1 scale by a linear transformation. The worst case disutility has the value 1 for full impact of the PM and the least case disutility has the value 0 for no impact on the PM. Table 3-3 shows the constructed scale for physical property damage including the disutility weights.

Level	Description	disutility
3	Catastrophic physical property damage, Greater than SR 10 million	1.00
2	Major physical property damage SR 1 million to SR 10 million	0.27
1	Minor physical property damage Less than SR 1 million.	0.03
0	No physical property damage	0.00

Table 3-3: Preliminary Constructed Scale for Physical Property Damage with Wiegth.

## 3.2 Risk Analysis Model

In 2002, the National Infrastructure Protection Center (NIPC) issued the document entitled “Risk Management: An Essential Guide to Protecting Critical Assets” which is a guide which helps organizations identify weaknesses and which offers them a defendable method for selecting cost-effective countermeasures to protect their valuable assets [63]. Also, it emphasizes the communication of risks and

recommendations to the decision makers to improve the success rate of their organization. This guide is used as a risk analysis model for the assessment of CIs at JIC. This model is a decision analysis tool which assists the decision makers in evaluating the terrorism risk at JIC. This model has five steps: Asset Assessment, Threat Assessment, Vulnerability Assessment, Risk Assessment and Identification of Countermeasure Options, Figure 3-2.

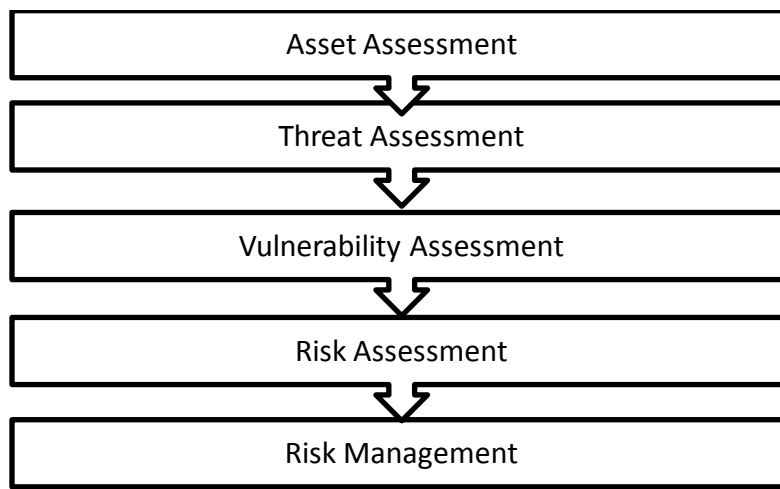


Figure 3-2 Risk Analysis Model [10].

### 3.2.1 Asset Assessment

This step is the most important step of the risk management process where all important assets are identified and prioritized. This step helps the decision makers to focus their resources on the most important assets. Some assets are tangible (e.g., people, facilities, equipment) while others are not (e.g., information, processes, reputation). In general CIs have two values; the value of the infrastructures themselves and their value as key assets. All the assets of petrochemical industries are provided in the next chapter.

### 3.2.2 Threat Assessment

The threat assessment step is related to the previous step. Threats can be identified by knowing the adversaries or events that can affect the previously identified assets. There are common types of adversaries such as criminals, hackers, foreign intelligence services, terrorists and others. However natural disasters and accidents are treated also as threats even though they do not possess intent [10], [63].

For this analysis of the petrochemical industry at JIC, we make use of six threat profiles.

These profiles are chosen to represent possible threats that might face petrochemicals industry at JIC. The six scenarios we examine are in Table 3-4.

Scenario	Profile	Type	Description
1	Major Threat	Malevolent action	<ul style="list-style-type: none"><li>· Caused by group or an individual with significant capability.</li><li>· Attack one or more plants.</li><li>· Result in damage requiring long term restoration (greater than 1 month) and causing significant impact on JIC industries.</li></ul>
2	Major Threat	Mechanical failure	<ul style="list-style-type: none"><li>· Caused due technical failure.</li><li>· One or more plants affected.</li><li>· Result in damage requiring long term restoration (greater than 1 month) and causing significant impact on JIC industries.</li></ul>
3	Moderate Threat	Malevolent action	<ul style="list-style-type: none"><li>· Caused by a capable group, or individual.</li><li>· Attack one or more plants.</li><li>· Result in damage requiring short term restoration (less than 1 month) and causing moderate impact on JIC industries.</li></ul>
4	Moderate Threat	Mechanical failure	<ul style="list-style-type: none"><li>· Caused due technical failure.</li><li>· One or more plants affected.</li><li>· Result in damage requiring short term restoration (less than 1 month) and causing moderate impact on JIC industries.</li></ul>
5	Minor Threat	Malevolent action	<ul style="list-style-type: none"><li>· Caused by group or individual with limited capability.</li><li>· One or more plants affected.</li><li>· Result in minor damage requiring minimal restoration (less than one week) and causing minor impact on JIC industries.</li></ul>
6	Minor Threat	Mechanical failure	<ul style="list-style-type: none"><li>· Caused due technical failure.</li><li>· One or more plants affected.</li><li>· Result in minor damage requiring minimal restoration (less than one week) and causing minor impact on JIC industries.</li></ul>

Table 3-4 Threat assessment scenarios for JIC

### 3.2.3 Vulnerability Assessment

Vulnerability is defined as any weakness in an entity to attack. The Vulnerability Assessment reviews the existing situation to understand the weaknesses in CIs. In CIs, susceptibilities may appear as lack of security patrols, guards, or security procedures. According to [10] susceptibilities can be classified into categories to assist the analyst in describing CIs, Table 3-5.

Level	Description
Extreme	Completely open, no controls, no barriers, unlocked
Very high	Unlocked, noncomplex barriers
High	Complex barrier, security patrols, video surveillance
Moderate	Secure area, locked, complex closure
Low	Guarded, secure area, locked, alarmed, complex closure
Very low	Completely secure, inaccessible

Table 3-5 Susceptibility Categories.

The vulnerability can also be expressed also as a function of the susceptibility to attack and the value of the assets.  $Vulnerability = f(Susceptibility, Value)$  [63]. [10] proposed vulnerability categories as shown in Table 3-6 and described in Table 3-7.

Susceptibility	Value					
	Extreme	High	Moderate	Low	Very low	Zero
Extreme	Red	Red	Orange	Yellow	Blue	Green
High	Red	Orange	Orange	Yellow	Blue	Green
Moderate	Orange	Orange	Yellow	Blue	Blue	Green
Low	Yellow	Yellow	Blue	Green	Green	Green
Very low	Blue	Blue	Green	Green	Green	Green
Zero	Green	Green	Green	Green	Green	Green

Table 3-6 Vulnerability categories [10].

Vulnerability	Description
Red	This category represents a severe vulnerability in the CI. It is reserved for the most critical locations that are highly susceptible to attack. Red vulnerabilities are those requiring the most immediate attention.
Orange	This category represents the second priority for counterterrorism efforts. These locations are generally moderately-to-extremely valuable and moderately-to-extremely susceptible.
Yellow	This category represents the third priority for counterterrorism efforts. These locations are normally less vulnerable because they are either less susceptible or less valuable than the terrorist desires.
Blue	This category represents the fourth priority for counterterrorism efforts.
Green	This is the final category for action. It gathers all locations not included in the more severe cases, typically those that are low (and below) on the susceptibility scale and low (and below) on the value scale. It is recognized that constrained fiscal resources are likely to limit efforts in this category, but it should not be ignored.

Table 3-7 Vulnerability Categories Description [10].

### 3.2.4 Identify Susceptibility to Different Threats

In this Thesis, we define the susceptibility as a threat-dependent variable. We have chosen to investigate the susceptibility to two different types of threats:

- A mechanical failure, corresponding to pipe breaks, plant failures.
- A malevolent action, such as vandalism or terrorism.

#### 3.2.4.1 Susceptibility to Mechanical Failure

We chose to work with a number of raw materials needed by each plant. The more raw material is needed the high probability of machine to fail. We classify the plants into six categories of susceptibility, as a function of the amount of raw materials needed by each plant. Table 3-8 presents the susceptibility categories taken into consideration for all JIC elements. The numbers indicate the category of susceptibility according to Table

3-9, ranging from 1 (low susceptibility) to 6 (high susceptibility). The same classification has been used for both links and nodes. We consider the input links as part of node elements. The susceptibility of each element is further detailed in Table 3-8.

Number of raw material	Number of nodes	JIC Elements	Rank	Susceptibility
1	2	Node 13, Node 14	1	Very Low
2	7	Node1, Node2, Node4, Node8, Node 9, Node 10, Node11, e11, e23, e12, e24, e14, e26, e18, e29, e19, e30, e20, e31, e21, e32	2	Low
3	1	Node 6, e6, e16, e27	3	Moderate
4	3	Node 3, Node 5, Node 7, e2, e4, e13, e25, e3, e5, e15, e35, e8, e17, e38, e36	4	High
5	0		5	Very High
>5	1	Node 12, e1, e7, e9, e10, e22, e33, e34	6	Extreme

Table 3-8 Susceptibility Categories for Mechanical Failures.

#### **3.2.4.2 Susceptibility to Malevolent Action**

Adapting Apostolakis and Lemon's approach [10], we define and use six qualitative levels of susceptibility to malevolent threats. The difficulty was to find a way to quickly assess the JIC's elements. The approach that seemed most sensible to both the author and the petrochemical industry was to link the susceptibility with the assets value. For example, it stands to reason that high-value assets are more susceptible to attack than low-value assets. Therefore the susceptibility was assessed simply by using the values of the assets and defining a generic susceptibility value for each of the categories.

As a result, Table 3-9 presents the susceptibility of JIC's elements to a "malevolent action" threat. The numbers indicate the assessed susceptibility ranging from 1

(low susceptibility) to 6 (high susceptibility). The same classification has been used for both links and nodes. We consider the input links as part of the node value.

Value in SR Million	Number of Nodes	JIC Elements	Rank	Susceptibility
<500	4	Node4, Node6, Node10, e6, e14, e16, e20, e26, e27, e31	1	Very Low
501-1000	2	Node3, Node5, e2, e3, e4, e5, e13, e15, e25, e35	2	Low
1001-1500	2	Node8, Node12, e1, e7, e9, e10, e18, e22, e29, e33, e34	3	Moderate
1501-2000	3	Node7, Node11, Node13, Node14, e8, e17, e21, e28, e32, e36	4	High
2001-2500	1	Node9, e19, e30	5	Very High
>2500	2	Node1, Node2, e11, e12, e23, e24	6	Extreme

Table 3-9 Susceptibility Categories for Malevolent Actions.

### 3.2.5 Risk Assessment

In this step, all the earlier assessments (asset, threat and vulnerability) are combined and evaluated in order to give a complete picture of the risks to the CIs. A prioritized list of all vulnerabilities in CIs is produced based on the value of the assets, the specified threat and the vulnerability of the CIs. The value tree and constructed scales are used to analyze CIs from specific threats. PI and susceptibility are compiled to produce a prioritized list for all items in CIs [10].

### 3.2.6 Identification of Countermeasure Options (Risk Management)

The objective of identifying countermeasure options is to lower the overall risk to CI to an acceptable level. According to [6], risk management builds on the risk assessment process by finding answers to the following questions:

- What can be done and what options are available?
- What are the trades-off in terms of costs, benefits and risks?
- What are the impacts of current management decisions on future operations?

The impact on each assessment for the CI must be reviewed for each countermeasure.

The risk assessment is repeated to account for the impact of the countermeasure. It is important to account for cost of the countermeasure and for any negative contribution the countermeasure may have to the overall risk [10]. For example, petrochemical plants depend on each other to get the required raw material. The output of plant A is an input for plant B. Usually one pipe only provides B with its raw material from A which is a single point of failure. To protect plant B, it might be recommended to back up this pipe. So that all the costs of providing such pipe must be calculated and taken into consideration. The overall cost may include the prior studies cost, implementation cost and security cost after implementation. All these cost must be considered

Risk Assessment is a continuous process to achieve success. It is not a one-off process. CIs should be monitored for any changes that could impact the analysis. Asset values may change; new threats may fade away and vulnerability may also change. Continuous assessment is necessary to timely efficiently and cost effectively address new risks [63].

### **3.3 Location-based Production Loss Calculation (LPLC)**

As we know, decision makers have a big concern about the expected loss resulting from terrorist attacks. Due to the nature of petrochemical industries, all plants are clustered in one area. We propose a methodology to calculate the loss in each plant within this



cluster. This methodology is called Location-based Production Loss Calculation (LPLC) which is based on node location. It is based on the distance between nodes and attack location. Also, it takes into consideration the direct or indirect connectivity with the target node.

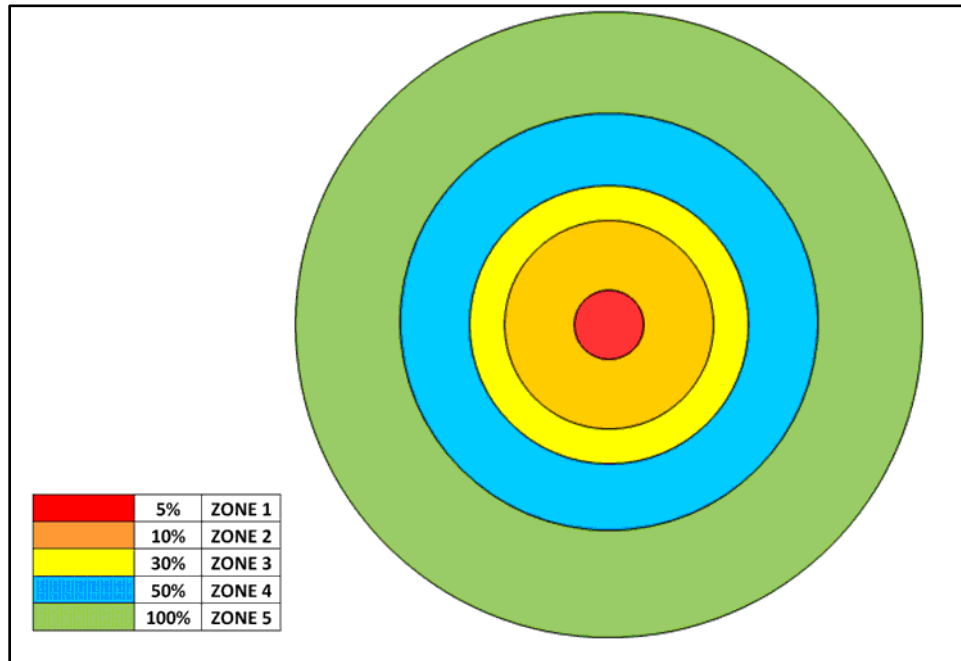


Figure 3-3 Area Coverage of Targeted Zones

This methodology divides the plant cluster into five zones as shown in Figure 3-3. The first zone covers 5% of the cluster area and starts from the attack location. All nodes in this zone will have Mean Time To Repair (MTTR) 2160 hours starting from the attack time. Also all nodes that connected to the nodes in this zone, belong to cut set nodes, will be suspended for the same period. The second zone covers 10% of the cluster area and has MTTR 720 hours. All zones are shown in Table 3-10. To test LPLC, three scenarios of terrorist attacks are used to test this methodology in the next Chapter.

Zone	Risk Value	MTTR	MTTR (H)	Explanation
1	5%	Three Months	2160	Major damages to the plant and large reconstruction is required
2	10%	One Months	720	Minor damages to the plant and some reconstruction is required
3	30%	One Week	168	Heavy maintenance is required and some equipments need replacement
4	50%	Three days	72	Heavy maintenance is required and some equipments repair
5	100%	12 Hours	12	No damages but light Maintenance Required for Safety

Table 3-10 LPLC Zones.

### 3.4 Proposed Methodology

The work of Apostolakis and Lemon (2005) is a systematic process to analyze failures in an infrastructure and rank them according to their impacts on the stakeholders. The work presented in this thesis extends their work and apply their methodology to petrochemical industry in Saudi Arabia in Jubail Industrial City (JIC) as follows:

- Apostolakis and Lemon considered a small community (MIT campus) and a small number of assets (buildings) that the decision makers wished to protect. This thesis considers a city (JIC) and all its petrochemical industry that the decision makers care about;
- A minimal cut set (MCS) approach is used to identify and analyze vulnerabilities in the CIs. Apostolakis and Lemon modeled the CIs using networks to take advantage of mathematical network analysis for the identification of minimal cut sets (MCS) [5]. In the petrochemical industry, the MCS is not the minimum edges

that disconnect the network. It goes beyond this and covers any edge(s) whose removal interrupts the petrochemicals production cycle;

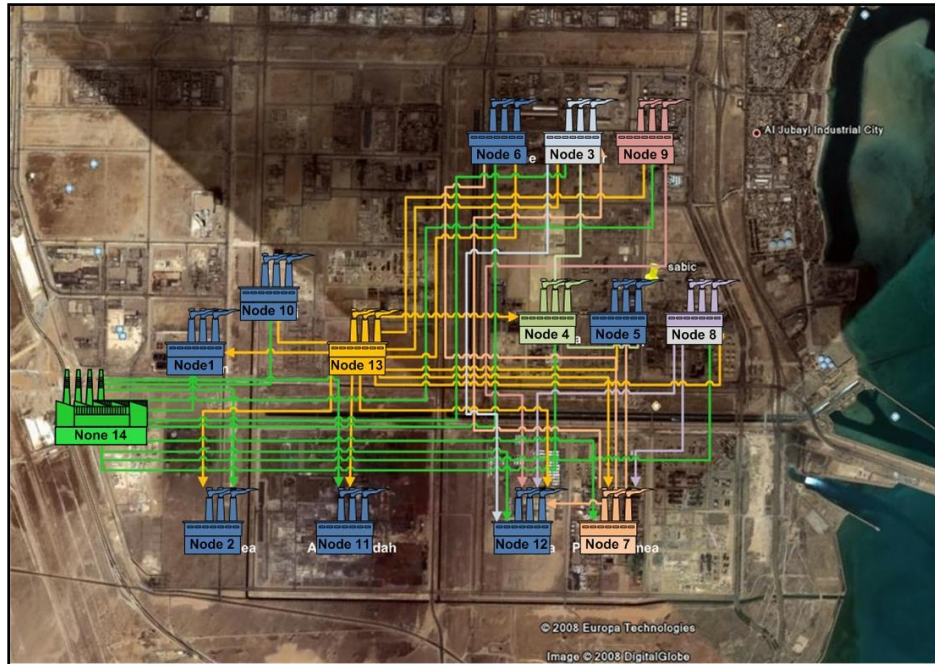


Figure 3-4 Petrochemical factories in JIC.

- All previous studies covered water-supply networks [38], natural gas network [39] and power grids [40]. In this work, we will apply this methodology to the petrochemical industry. The links in water, gas and power networks carry one material in each system. For example, in water-supply systems the material being transported over the network is only water. While in petrochemical industry the material that is carried over the network depends on the production needs of each plant.

- Due to the criticality of the in petrochemical industry, the capacity of the elements in the system is not taken into account. The system elements are modeled as binary (success–failure) items;
- Time is taken into account explicitly because the consequences of losing service is time-dependent; and
- The decision makers considered in this work are five decision-makers in the petrochemical industry in Saudi Arabia.
- This study analyzes the physical and geographical interdependencies in petrochemical plants in JIC. The physical interdependency applied to plants that depend on the products of other plants. Any failure or disruption to any source plant results in the failure of the receiving plants. The geographical interdependency occurs due to the widespread location of petrochemical plants at JIC where 14 plants cover approximately 80 km, as shown in Figure 3-4. These plants are connected together via a network of pipes which is more than 150 km long. For security reasons, these data have been partially modified and do not represent the real petrochemical industry in JIC.
- Due to the nature of petrochemical industries where all plants are clustered in a large area, a new methodology is proposed to estimate the loss due terrorist attacks. Any attach to this cluster affect all plants either directly or indirectly. This methodology calculates the loss based on the plants location within the petrochemical cluster.

## **Chapter Four: Petrochemical Industry at JIC Case Study**

### **4.1 Background**

After September 11, 2001, the East Coast blackout of August 14, 2003 and the 7 July 2005 London bombings, CIs protection (CIP) became a world focus. Terrorist acts are aimed for maximum social disruption. One subset of the potential targets of terrorist acts is the nation's CIs [6]. These CIs include telecommunications, energy, industrial plants, banking and finance, transportation, water systems, emergency services at both the governmental and private levels. They are complex and interdependent and sensitive to disruptions that can lead to cascading failures with serious consequences. Complex CIs have critical nodes and any attack on these nodes could lead to a significant disruption.

Computerization and automation used to improve the efficiency of many CIs, have resulted in an increase in system complexity, and dependency [65], [66]. According to [26] interdependency can be defined as a bidirectional relationship between two CIs through which the state of each CI influences the state of the other and vice-versa. Due to these technical complexities and a general lack of understanding of interdependent relationships among CIs, CI interdependencies are considered to be a weakness and may permit vulnerabilities to go unrecognized until a major failure occurs to the CIs.

## 4.2 Petrochemical Industry CI

The petrochemical industry is considered as one of the major CI in any oil-producing country. It uses oil and natural gas as major raw materials to produce chemicals. Petrochemicals can be converted into thousands of industrial and consumer products, including plastics, paints, rubber, fertilizers, detergents, dyes, textiles and solvents. This industry consists of two major divisions. The first one is the primary petrochemical industry which produces basic chemicals, such as ethylene, from oil or gas. The second one is the secondary industry which converts the basic petrochemicals into materials that may be directly used by other industries [67].

From a security perspective, chemical facilities could be converted into weapons of mass destruction. For example there are about 600 facilities in the US which could each potentially threaten between 100,000 and a million people and about 2,300 facilities which could each potentially threaten between 10,000 and 100,000 people within these facilities' "vulnerable zones" [68]. Also, the chemical manufacturing industry supplies other industries with key products (agriculture, pharmaceuticals, drinking water and food processing) [69]. In general, a failure in CI will have a significant impact on another sector which performs necessary functions. So any attack on a petrochemical facility could disrupt the economy or seriously impact other CIs. The majority of experts in the chemical industry agree that the chemical facilities are attractive targets for terrorists [69]. Also, they believe that current security conditions at most chemical facilities are inadequate [70].



Figure 4-1: Map of Kingdom of Saudi Arabia.

### 4.3 Petrochemical Industry at JIC

This thesis focuses on the petrochemical industry in Jubail Industrial City (JIC) in Saudi Arabia, (Figure 4-1). JIC is considered as the centre for future national economic growth by the Saudi Government. It is an international hub for value-added petrochemical industry and an increasingly recognized destination for real estate investment. JIC is located in the Eastern province of Saudi Arabia and its population is about 250,000 people [71]. It was designated as a new industrial city by the Saudi government, and has seen rapid expansion and industrialization since. It is a complex of petrochemical plants, iron works and a number of smaller companies, plus a Royal Saudi Naval Base. It is also

considered as the Middle East's largest and the world's 5<sup>th</sup> largest petrochemical company, Saudi Basic Industries Corp. (SABIC) [72]. Also it is home to the world's largest seawater desalination plant. It provides 50% of the country's drinking water through desalination of the water from the Arabic Gulf. King Fahd Industrial Port, in JIC, is used for different import and export needs. In JIC, there are more than 20 factories of primary industries and more than 25 factories of secondary industries [71].

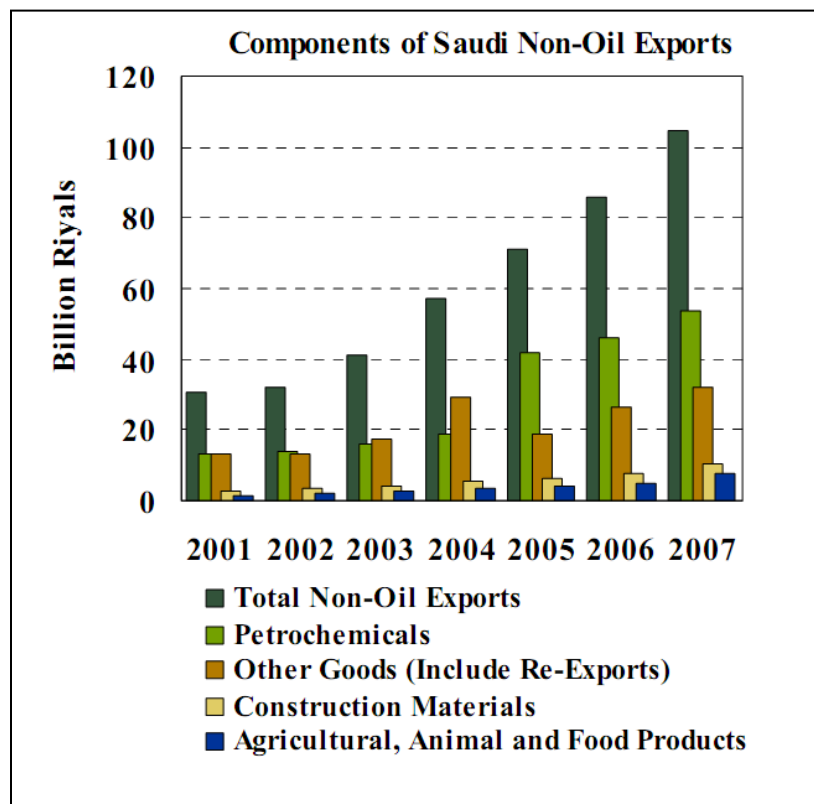


Figure 4-2: Components of Saudi Non-oil Exports [73].

Saudi Arabia is considered as a key player in the global petrochemical industry. It accounts for 75% of GCC petrochemical production [74]. Figure 4-2 shows that petrochemical production accounts for about one half of Saudi non-oil exports [73]. The petrochemical industry in Saudi Arabia enjoys a natural competitive advantage due to



the availability of low cost feedstock on account of the vast crude oil and natural gas resources. Estimates are that more than \$70 billion of petrochemical projects are currently under development in the Kingdom. The Saudi Arabian Oil Company (Saudi Aramco) is also forging ahead with its own plans to be a serious player in the downstream petrochemical sector. It has entered the industry with a \$16 billion Ras Tanura project that envisages 1.2 million tons per year ethane/naphtha cracker, 400,000 tons per year of propylene, 400,000 tons per year of benzene, 460,000 tons per year of paraxylene and a polyolefin mix unit. Aramco and Dow are discussing a joint development of this project. Work is also under way at full speed on the world's largest integrated \$9.8 billion plus Petro-Rabigh complex. This is a joint venture between Saudi Aramco and Sumitomo Chemical Company of Japan. The project is expected to come on stream by mid-2008. The plant will have the capacity to produce 600,000 tons per year of mono-ethylene glycol (MEG) and 200,000 tons per year of propylene oxide (PO) [74], [73].

#### **4.4 JIC Value Tree and User Performance Index (PI) Assessment**

As it is mentioned earlier, JIC consists of 14 plants to produce different petrochemical materials these plants are connected together via 36 pips (links), see Table 4-1. Core materials, Gas and Oil, are taken from Node 13 and Node 14. However some factories take the output of other factories as input, physical dependency.

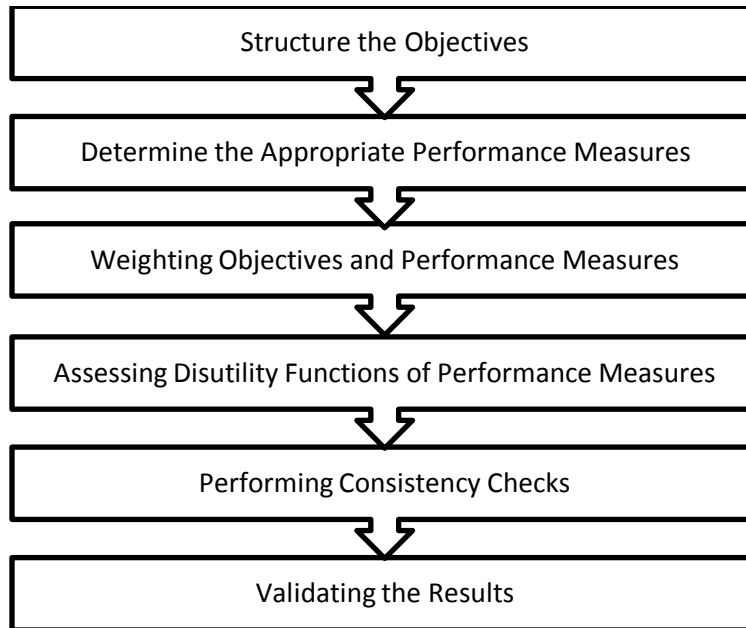
Plant	Product	Raw Materials	Source
Node 1	Methanol	Gas	Node 14
	Butanediol	Butene	Node 14
Node 2	Poly Propylene	Gas	Node 13
		Propene	Node 14
Node 3	MTBE	Butane	Node 14
	Poly Propylene	Methynol	Node 4
		Propylen	Node 7
Node 4	Menthol	Methan	Node 14
	MTBE	Butane	Node 14
Node 5	Polyethylene	Ethylene	Node 7
	Ethylene Glycol	Butene	Node 7
		Oxagen	Node 13
		IC	Node 4
Node 6	Ammonia	Gas	Node 14
	Ethyl hexanol	Propylene	Node 7
Node 7	ethylene	Dichloride Ethylene	Node 8
	Propylene	Sodium Hydroxide	Node 8
	Butene	Propan	Node 14
		Methan	Node 14
		Ethan	Node 14
Node 8	ethylene	Ethan	Node 14
	Sodium Hydroxide	Benzene	Node 14
	Ethylene Dichloride	Methan	Node 14
		Methyanol	Node 14
		Butane	Node 14
Node 9	fertilizer	Methan	Node 14
Node 10	Methanol	Gas	Node 14
Node 11	ethylene	Ethan	Node 14
	Monoethylene Glycol	Methan	Node 14
Node 12	Ethylene	Butene	Node 7
	Propylene	Iso Bentene	Node 3
	Bi-Node 13	Ethylene	Node 8
	LLDPE	Ethylene	Node 7
	LDPE	Questic	Node 8
		Ethan	Node 14
		Selferic-Acid	Node 9
		Netrogene	Node 13
Node 13			
Node 14			

Table 4-1 Input and Output Quantity for JIC Factories.

Our approach is based on a performance index (PI) to determine the priority for each item in CI [10]. The item with higher PI has the higher priority. The PI is calculated by summing the weight of individual performance measures (PM) multiplied by the utilities of each item in CI. The PMs are measures of CI's objectives. The PI is calculated by this equation:

$$PI_j = \sum_i^{K_{pm}} w_i u_{ij} \quad (2)$$

Where  $PI_j$  is the performance index for item  $j$ ,  $w_i$  is the weight of PM  $i$ ,  $u_{ij}$  is the utility of PM <sub>$i$</sub>  for item  $j$  and  $K_{pm}$  is the number of PMs. According to [7], there are six steps to determine the PIs:



#### 4.4.1 Step 1: structuring the objectives

The first step to determine the PIs is the structuring of objectives to be satisfied. Before structuring the objectives, we held interviews with 5 decision makers, DM1, DM2, DM3,

DM4 and DM5, who have different background in petrochemical industries. In each interview we explained to the decision makers the intent and the structure of the methodology applied in this research. In order to assist them to structure the objectives, a set of fundamental objectives that are applicable in a wide variety of prioritization contexts is presented [58]. These objectives are not exhaustive, but intended to guide the decision maker in to identify fundamental objectives. The objectives are shown in Table 4-2.

Objective	Explanation
Economic	Accounts for costs and include economic impact on own property and other people's property.
Health and Safety	Accounts for risks to workers and the public
External relationships	Accounts for damage to relationships with general public, customers and workers.
Environment	Accounts for the impact on the environment

Table 4-2 Main objectives proposed for decision makers.

According to [59], [75], value tree can be used to help in structuring objectives and PMs. We showed the decision makers a preliminary value tree and we asked them what they do when they prioritize items and what they feel are important considerations. Using one interview as a springboard for another, we developed the value tree for JIC as shown in Figure 4-3 which is a result of several iterations between us and decision makers. There are four broad categories of impacts: health and safety, the company's image, the economic and the environment. The next tier of the tree in Figure 4-3 shows the PMs that help to quantify impact categories.

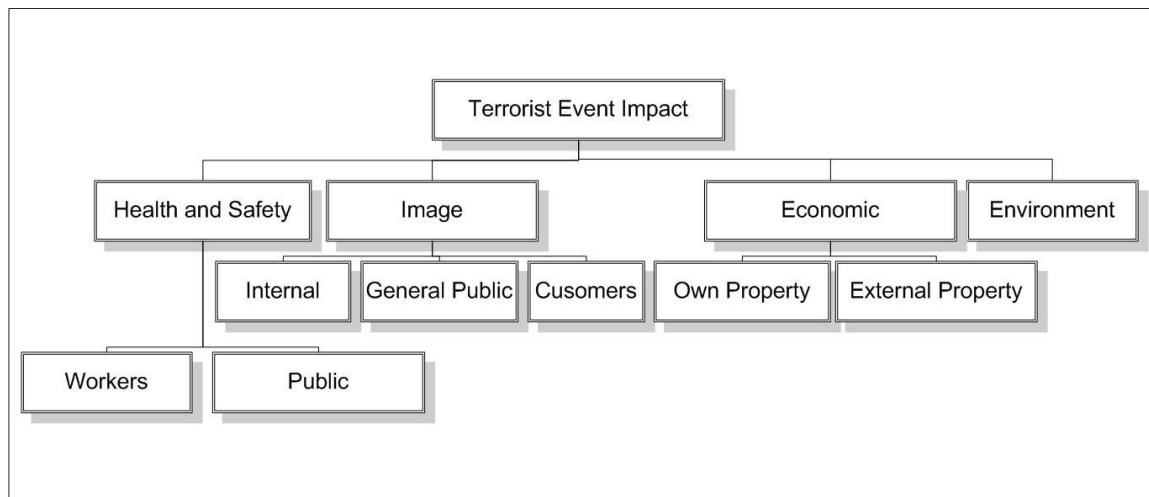


Figure 4-3 JIC value tree.

#### 4.4.2 Step 2: determine appropriate performance measures

Performance Measures (PMs) are used to test the extent to which each objective is satisfied. The decision makers identify appropriate PMs for their value tree. Then, they have to agree on appropriate measurement instruments. These instruments could be natural metrics such as dollars for an economic objective, or constructed scales which are linguistic scales separated into different levels of impact and each level has a description to each level [58].

Due to the limited time for each interview with the decision makers, we used the constructed scales in [10] to be primary constructed scales in this work. After that it is shown to the decision makers for feedback. After reviewing all the feedbacks, the final constructed scales for JIC produced are shown in Table 4-3, Table 4-4, Table 4-5 and Table 4-6.

	Workers
Level	Constructed Scale
4.00	A large share of the served population requires treatment
3.00	Hundreds of persons require treatment, dozens of them hospitalization.
2.00	Dozens of persons require treatment, some of them hospitalization
1.00	A few persons require light treatment.
0.00	No health impact
	Public
Level	Constructed Scale
4.00	A large share of the served population requires treatment.
3.00	Hundreds of persons require treatment, dozens of them hospitalization.
2.00	Dozens of persons require treatment, some of them hospitalization.
1.00	A few persons require light treatment.
0.00	No health impact.

Table 4-3 Constructed Scales for Safety and Health

	Internal Image
Level	Constructed Scale
4.00	Responsibility is taken away to Ministry of Interior/political institutions.
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.
2.00	A written report is required by Eastern Region Governor/political institutions to explain incidents.
1.00	Verbal enquiry from Eastern Region Governor.
0.00	No negative image.
	Image with the General Public
Level	Constructed Scale
4.00	International interest from the media.
3.00	Repeated appearance in national media appearance in international media.
2.00	Repeated publication in local media, appearance in national media
1.00	Single appearance in the local media
0.00	No negative image with the General Public
	Image with Customers
Level	Constructed Scale
4.00	Most critical customers upset
3.00	Numerous letters from different customers
2.00	Repeated verbal communications, few letters
1.00	Few verbal communications
0.00	No negative image

Table 4-4 Constructed Scales for Image

	Economic Impact on Own Property
Level	Constructed Scale
4.00	Dozens of Millions of Saudi Riyals.
3.00	Millions of Saudi Riyals.
2.00	Hundreds of thousands of Saudi Riyals.
1.00	Dozens of thousands of Saudi Riyals.
0.00	No economic impact.
	Economic Impact on Other People's Property
Level	Constructed Scale
4.00	Dozens of Millions of Saudi Riyals.
3.00	Millions of Saudi Riyals.
2.00	Hundreds of thousands of Saudi Riyals.
1.00	Dozens of thousands of Saudi Riyals.
0.00	No economic impact.

Table 4-5 Constructed Scales for Economic

	Impact on the Environment
Level	Constructed Scale
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems
2.00	Medium environmental damage, with some animals perishing. Eventually reversible
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems
0.00	No environmental impact.

Table 4-6 Constructed Scales for Environment

#### 4.4.3 Step 3: weighing objectives and performance measures

After constructing the value tree and identifying the PMs, we asked five decision makers, DM1, DM2, DM3, DM4 and DM5, to assign weights to the PMs using the Analytic Hierarchy Process (AHP) [75], [61]. It is a decision-making technique developed by Thomas L. Saaty in the 1970s [61]. It is a method of breaking down a complex, unstructured situation into its components parts; arranging these parts, or judgments on the relative importance of each variable; and synthesizing the judgments to

determine which variables have the highest priority and should be acted upon to influence the outcome of the situation [61]. Since we have already structured the value tree in a hierarchical arrangement, decision maker can apply AHP straightforward. First, decision maker make pairwise comparisons of the impact categories with respect to the overall goal. Then, the decision makers compare the next lowest level of objectives to the objective above it. This is repeated until the PMs get their weights.

For example, there are two PMs for the impact category Health and Safety: the number of worker suffering health effects and the number of external people suffering health damage that may be caused by the terrorist attack.

To start the weighing process, we asked the decision makers compare one objective to another objective with respect to the overall goal. For example, looking at Figure 4-4, DM1 compared the *economic* to the *image* with respect to the overall goal of terrorist event impact. In this case, DM believed that *economic* is strongly important than *image* (as indicated by the fact that he circled *economic* and wrote 7 in the space provided).



Instructions:

A. Compare the two items listed; circle the item that you feel is the most important.

B. Indicate how much more important the circled item is using the scale provided:

1 – equally    3 – weakly    5 – moderately    7 – strongly    9 – extremely Use even numbers to indicate importance between these increments.

**Impact Categories**

1. Economic vs. Image	( <u>  7  </u> )
2. Economic vs. Health & Safety	( <u>  7  </u> )
3. Image vs. Health & Safety	( <u>  9  </u> )
4. Environment vs. Economic	( <u>  3  </u> )
5. Environment vs. Health & Safety	( <u>  5  </u> )
6. Environment vs. Image	( <u>  9  </u> )

Figure 4-4 Example of DM1's relative importance assessment

As a result of this comparison, a seven appears in row 4 column 3 of the matrix of DM's comparisons shown in Table 4-9. Furthermore, 0.1429, or the reciprocal of 7 is shown in row 3 column 4 of the matrix of comparisons. The remainder of the entries of the matrix of comparisons was populated in a similar way.

Figure 4-5 shows the relative weights of DM1 for the impact categories and the PMs. Clearly, the DM1 value Health and Safety (weight: 0.6021) much higher than the remaining three categories (weights: 0.0360, 0.2037 and 0.1582). These weights were elicited by DM1 using the analytic hierarchy process (AHP) [61].

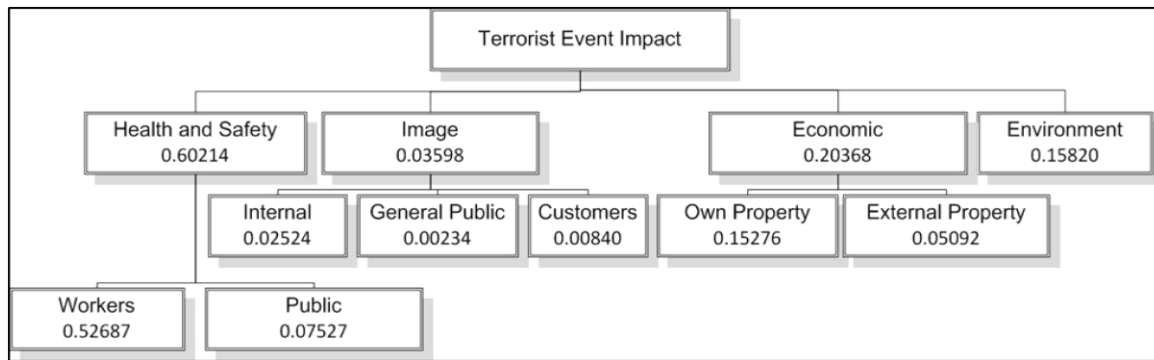


Figure 4-5 Constructed weight of the value tree for DM1.

Table 4-7 shows the initial constructed weight of the value tree for the five decision makers.

	DM1		DM2		DM3		DM4		DM5	
<b>Impact Category</b>	Local Weight	Global Weight	Local Weight	Global Weight	Local Weight	Global Weight	Local Weight	Global Weight	Local Weight	Global Weight
<b>Health and Safety</b>	0.4291	0.4291	0.0534	0.0534	0.0580	0.0580	0.1057	0.1057	0.5143	0.5143
Workers	0.8750	0.3754	0.8000	0.0427	0.8750	0.0508	0.8750	0.0925	0.8333	0.4286
Public	0.1250	0.0536	0.2000	0.0107	0.1250	0.0073	0.1250	0.0132	0.1667	0.0857
<b>Image</b>	0.0501	0.0501	0.1750	0.1750	0.0940	0.0940	0.2162	0.2162	0.1158	0.1158
Internal	0.5364	0.0269	0.0675	0.0118	0.4353	0.0409	0.1580	0.0342	0.2157	0.0250
General	0.0800	0.0040	0.1463	0.0256	0.0782	0.0074	0.7311	0.1581	0.0612	0.0071
Customers	0.3836	0.0192	0.7861	0.1376	0.4866	0.0458	0.1109	0.0240	0.7231	0.0838
<b>Economic</b>	0.3184	0.3184	0.6667	0.6667	0.4396	0.4396	0.0547	0.0547	0.3045	0.3045
Owned Property	0.7500	0.2388	0.1111	0.0741	0.5000	0.2198	0.8750	0.0478	0.1250	0.0381
External Property	0.2500	0.0796	0.8889	0.5926	0.5000	0.2198	0.1250	0.0068	0.8750	0.2664
<b>Environment</b>	0.2024	0.2024	0.1049	0.1049	0.4083	0.4083	0.6234	0.6234	0.0654	0.0654

Table 4-7 Initial constructed weight of the value tree for the five decision makers.

After the decision makers completed their initial assessments, their results are tested using the consistency index and the consistency checks in AHP. These inconsistencies may happen because of many reasons e.g. the pairwise comparisons elicit redundant information. Table 4-8 shows the initial matrix of comparisons for DM1. After identifying

inconsistencies we asked the decision makers to reassess their preferences. After attaining satisfactory consistency, the decision makers approved the final weights.

	Health and Safety	Image	Economics	Environment
Health and Safety	1	9	7	5
Image	0.1111	1.00	0.1429	0.1111
Economics	0.1429	7	1	3
Environment	0.2000	9	0.3333	1
Weights	0.6021	0.0360	0.2037	0.1582

Table 4-8 DM1's initial matrix of comparisons.

After the entire matrix of comparisons was populated, we computed the consistency index for DM's initial comparison. In DM1's case the consistency index was 0.326 which is not as consistent as we would usually like, it is acceptable Saaty [61]. After revising for consistency the weights shown in Table 4-9 were produced. The original weights were 0.6021 for *safety*, 0.036 for *image*, 0.2037 for *economic* and 0.1582 for *Environment*. We showed DM1 his initial weights and the revised weights and he accepted those results.

Rank	Impact Category	Weight
1	Health and Safety	0.4291
2	Economic	0.3184
3	Environment	0.2024
4	Image	0.0501

Table 4-9 DM1's ranking of objectives and weights

Table 4-10, Table 4-11, Table 4-12 and Table 4-13 show the final objective weight ranking table for DM2, DM3, DM4 and DM5. All theses tables are passed through the same procedure that we have done for DM1 table. We can notice that each decision

maker has different ranking. DM1 and DM5 have health and safety at rank 1 while DM2 and DM3 rank it 4. These differences are related to the background of the decision makers and their ways for prioritizing these objectives. This diversity assists this research to cover different decision makers' attitudes.

Rank	Impact Category	Weight
1	Economic	0.6667
2	Image	0.1750
3	Environment	0.1049
4	Health and Safety	0.0534

Table 4-10 DM2's ranking of objectives and weights.

Rank	Impact Category	Weight
1	Economic	0.4396
2	Environment	0.4083
3	Image	0.0940
4	Health and Safety	0.0580

Table 4-11 DM3's ranking of objectives and weights.

Rank	Impact Category	Weight
1	Environment	0.6234
2	Image	0.2162
3	Health and Safety	0.1057
4	Economic	0.0547

Table 4-12 DM4's ranking of objectives and weights.

Rank	Impact Category	Weight
1	Health and Safety	0.5143
3	Economic	0.3045
2	Image	0.1158
4	Environment	0.0654

Table 4-13 DM5's ranking of objectives and weights.

#### 4.4.4 Step 4: assessing utility functions of PMs

After structuring the value tree, determining the PMs and assigning weights to those PMs, the decision maker assesses their utility functions. Once complete, the decision maker will have all of the information needed to calculate a performance index for each JIC item. To assess the utility function for PMs, we use AHP again because the decision maker is already familiar with this technique. It is nearly identical to the weighting of objectives and PMs. The decision maker performs pairwise comparisons for each constructed scale between the different levels of the constructed scale with respect to the objective above the PM on the value tree. Then these comparisons are converted into weights where each level will have a weight assigned to it. After that all weight are revised for consistency as what we did in previous section.

As we mention earlier in step 2 regarding to the limited number of interviews with the decision makers the utility value for constructed scales are unified to be used for all the decision makers. Also, a primary utility values are shown to the decision makers to have feedbacks. The final utility values are approved after several iterations. Table 4-14, Table 4-15, Table 4-16 and Table 4-17 show the utility values for all constructed scales.

	Workers	
Level	Constructed Scale	Utility
4.00	A large share of the served population requires treatment.	1
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881
1.00	A few persons require light treatment.	0.0591

0.00	No health impact	0
	Public	
Level	Constructed Scale	Utility
4.00	A large share of the served population requires treatment	1
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881
1.00	A few persons require light treatment.	0.0591
0.00	No health impact	0

Table 4-14 Constructed Scales for Safety and Health with Utility Value.

	Internal Image	
Level	Constructed Scale	Utility
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.00
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.45
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.13
1.00	Verbal enquiry from Eastern Region Governor	0.04
0.00	No negative image	0.00
	Image with the General Public	
Level	Constructed Scale	Utility
4.00	International interest from the media.	1
3.00	Repeated appearance in the national media appearance in the international media.	0.4092
2.00	Repeated publication in the local media, appearance in the national media	0.1363
1.00	Single appearance in the local media	0.0374
0.00	No negative image with the General Public	0
	Image with Customers	
Level	Constructed Scale	Utility
4.00	Most critical customers upset	1
3.00	Numerous letters from different customers	0.3905

2.00	Repeated verbal communications, few letters	0.1658
1.00	Few verbal communications	0.0573
0.00	No negative image	0

Table 4-15 Constructed Scales for Image with Utility Value.

Economic Impact on Own Property		
Level	Constructed Scale	Utility
4.00	Dozens of Millions of Saudi Riyals	1
3.00	Millions of Saudi Riyals	0.3697
2.00	Hundreds of thousands of Saudi Riyals	0.1311
1.00	Dozens of thousands of Saudi Riyals	0.0441
0.00	No economic impact	0.00
Economic Impact on Other People's Property		
Level	Constructed Scale	Utility
4.00	Dozens of Millions of Saudi Riyals	1
3.00	Millions of Saudi Riyals	0.3697
2.00	Hundreds of thousands of Saudi Riyals	0.1311
1.00	Dozens of thousands of Saudi Riyals	0.0441
0.00	No economic impact	0

Table 4-16 Constructed Scales for Economic with Utility Value.

Impact on the Environment		
Level	Constructed Scale	Utility
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems	1
2.00	Medium environmental damage, with some animals perishing. Eventually reversible	0.2842
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems	0.0686
0.00	No environmental impact	0

Table 4-17 Constructed Scales for Environment with Utility Value.

#### 4.4.5 Step 5: performing consistency checks

In order to ensure that the weights are correct, we must perform consistency checks for all constructed scales [58], [75]. A consistency check compares the absolute contribution from a performance measure to the contribution from the other performance measures. When making these comparisons, it is often useful to compare the maximum values of the performance measures to each other.

For example, compare the DM's preferences between own property damage and impact on the environment. The contribution to the overall assessment from each PM is the product of the weights of the PM and the disutility from the constructed scale. Comparing major physical property damage with a minor environmental impact reveals the contribution from each PM to the overall goal to be equal:

For DM1:

$$PI(\text{own property damage}) = \text{weight}(0.2388) * \text{disutility}(0.3697) = 0.0883$$

$$PI(\text{environmental impact}) = \text{weight}(0.2024) * \text{disutility}(0.0686) = 0.0139$$

For DM2:

$$PI(\text{own property damage}) = \text{weight}(0.0741) * \text{disutility}(0.3697) = 0.0274$$

$$PI(\text{environmental impact}) = \text{weight}(0.1049) * \text{disutility}(0.0686) = 0.0072$$

For DM3:

$$PI(\text{own property damage}) = \text{weight}(0.2198) * \text{disutility}(0.3697) = 0.0813$$

$$PI(\text{environmental impact}) = \text{weight}(0.4083) * \text{disutility}(0.0686) = 0.2800$$

For DM4:

$$PI(\text{own property damage}) = \text{weight}(0.0478) * \text{disutility}(0.3697) = 0.0177$$

$$PI(\text{environmental impact}) = \text{weight}(0.6234) * \text{disutility}(0.0686) = 0.0428$$



For DM5:

PI (own property damage) = weight (0.0381) \* disutility (0.3697) = 0.0141

PI (environmental impact) = weight (0.0654) \* disutility (0.0686) = 0.0045

These results show that DM1, DM2, DM4 and DM5 agreed on major impact on own property has higher priority than minor impact on environment. While DM3 result shows minor impact on environment has high priority than major impact own property. These results are shown to all decision makers to let them adjust the value tree weights and constructed scales disutility values until consistency is satisfied.

## 4.5 Network Analysis

Apostolakis and Lemon in [10] applied the MCS technique which is based on graph theory to find all the minimum cut set. In this thesis we found that MCS technique is applicable only in homogenous networks such as water supply network and power grid networks. However it is not applicable for heterogeneous networks such as petrochemical industry network. To solve this issue, we proposed a new technique to find the minimum cut set for both types of networks, homogenous and heterogeneous. This technique is called Production Minimum Cut Set (PMCS). It has two parts: PMCS for nodes which find the set of nodes that are affected by node removal and PMCS for links which find the set of nodes that we affected by link removal.

### 4.5.1 Production Minimum Cut Set (PMCS) for Node

Every node belong to a digraph network has input and/or output links. Let's call the input links "*Requirements*". These *Requirements* sets are known for each node. The

algorithm for this technique starts by deleting one node at a time from the network and delete all the output links of this node. Then, we compare the *Requirements* set for each nodes with its input. The comparison here is based on type not based on the number of links. For example, if *Requirement* set for a node is {gas, petrol, oxygen} and input set is {gas, petrol, gas, oxygen}, that means the node is connected. But if *Requirement* set for a node is less than the input set that means the node is disconnected. For example, if Requirement set {gas, petrol, oxygen} and input set is {gas, gas, oxygen}, that means the node is disconnected. For each node we make a list where this node is part of the cut set of this list of nodes. Figure 4-6 shows chart of this technique.

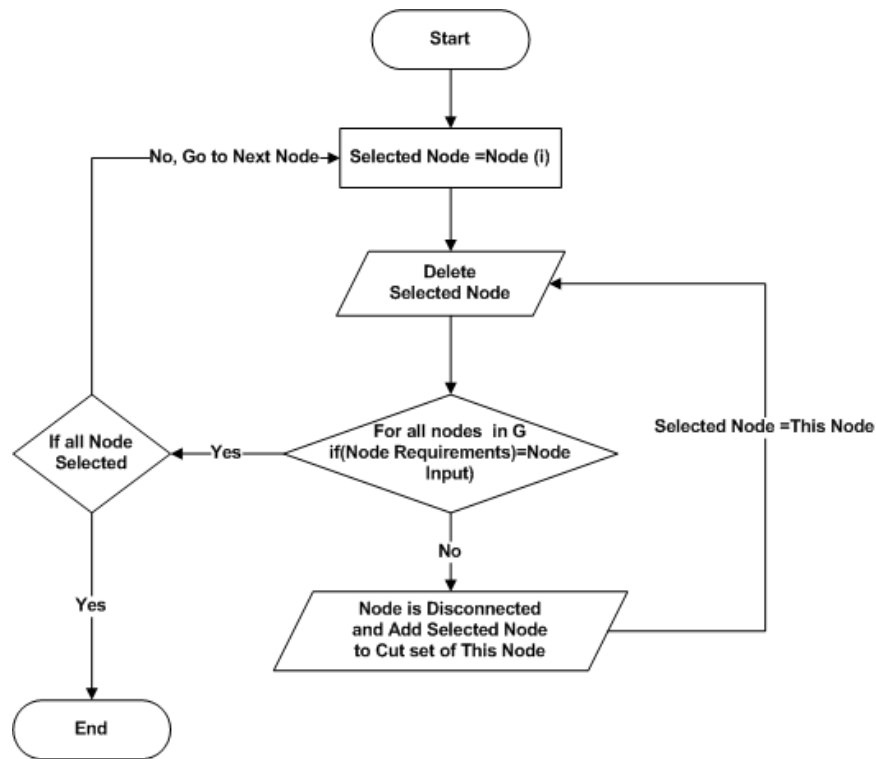


Figure 4-6 PMCS Algorithm for Nodes.

#### 4.5.2 Production Minimum Cut Set (PMCS) for Link

This part is similar to the node technique but in each loop we are deleting one link at a time. Each link will have a set of nodes that it affected by its removal. This link is considered as a member of the cut set of each effected node. Figure 4-7 shows the algorithm used in PMCS.

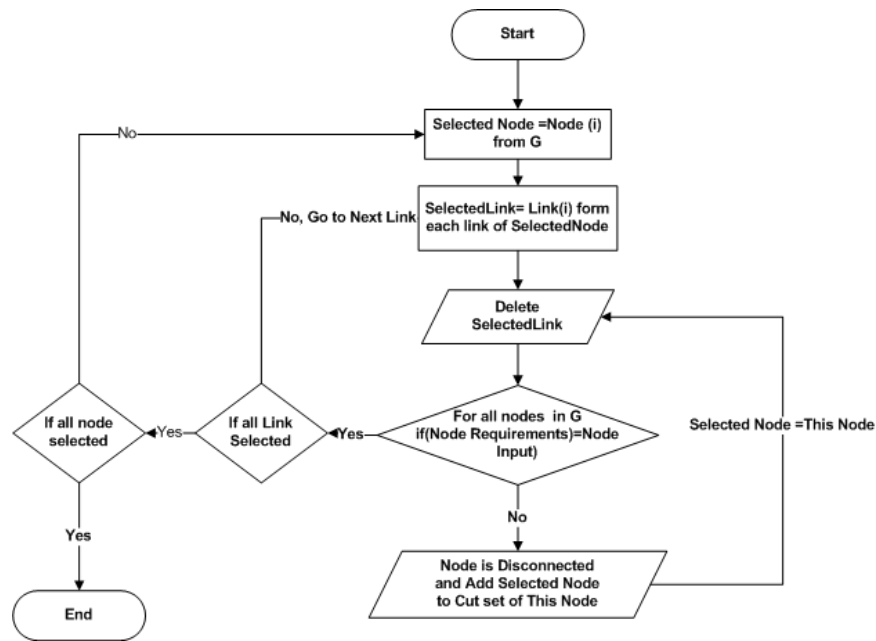


Figure 4-7 PMCS Algorithm for Link.

Production Minimum Cut Set (PMCS) of petrochemical industry network at JIC as the follow:

PMCS (Node1) = {Node 1, Node 13, Node 14, e11, e23};

PMCS (Node2) = {Node 2, Node 13, Node 14, e12, e24};

PMCS (Node3) = {Node 3, Node 4, Node 7, Node 8, , Node 13, Node 14, e2, e4, e8, e13, e14, e17, e18, e25, e26, e28, e29 ,36};

PMCS (Node4) = {Node4, Node 13, Node 14, e14, e26};

PMCS (Node5) = {Node 4, Node 5, Node 7, Node 8, Node 13, Node 14, e3, e5, e8, e14, e15, e17, e18, e26, e28, e29, e35, e36};

PMCS (Node6) = {Node 6, Node 7, Node 8, Node 13, Node 14, e6, e8, e16, e17, e18, e27, e28, e29, e36};

PMCS (Node7) = {Node 7, Node 8, Node 13, Node 14e, 8, e17, e18, e28, e29, e36};

PMCS (Node8) = {Node8, Node 13, Node 14, e18, e29};

PMCS (Node9) = {Node9, Node 13, Node 14, e19, e30};

PMCS (Node10) = {Node10, Node 13, Node 14, e20, e31};

PMCS (Node11) = {Node11, Node 13, Node 14e, 21, e32}

PMCS (Node12) = {Node 3, Node 4, Node 7, Node 8, Node 9, Node 12, Node 13, Node 14, e1, e2, e4, e8, e10, e13, e14, e17, e18, e19, e22, e25, e26, e28, e29, e30 e33, e34, e36}

PMCS (Node 13) = {Node 13};

PMCS (Node 14) = {Node 14}.

#### 4.5.2.1 Scenarios types

As it is mentioned earlier, we are going to test JIC element based on six scenarios. The first three are terrorist attacks scenarios while the others are machine failures scenarios.

##### 4.5.2.1.1 Terrorist attack scenarios

Table 4-18 shows the details of the terrorist attack scenarios. These types of scenarios are combine both location of nodes and the effected node based on the PMCS cut sets.

Scenario	Type	Target Node	Effected Node
1	Major	Node 8 and Node 5	Node3, Node5, Node6, Node7, Node8, Node12
2	Moderate	Node 10 and Node 1	Node1, Node10
3	Minor	Node 7 and Node 12	Node3,Node5,Node6,Node7,Node12

Table 4-18 Terrorist attack scenarios.

Any attack will affect its neighborhood nodes and its connected nodes. Figure 4-8, Figure 4-9 and Figure 4-10 shows these scenarios.

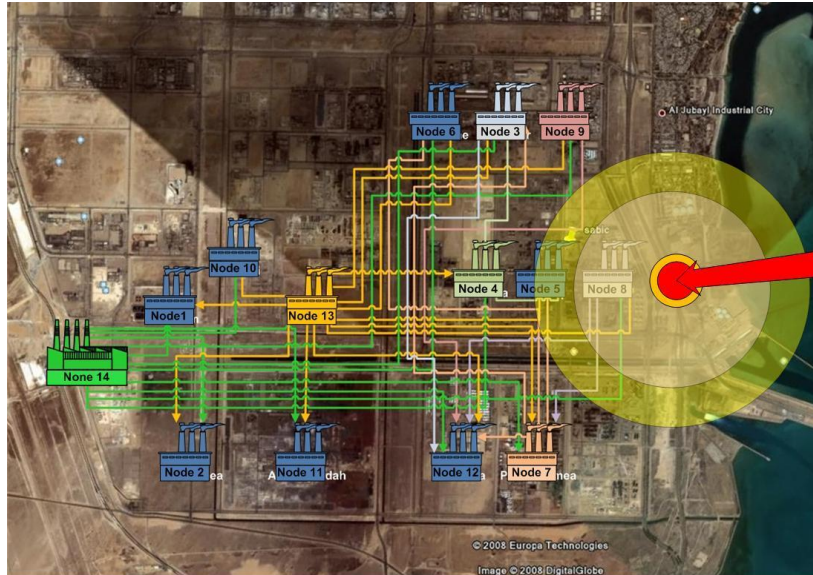


Figure 4-8 Scenario 1 location.

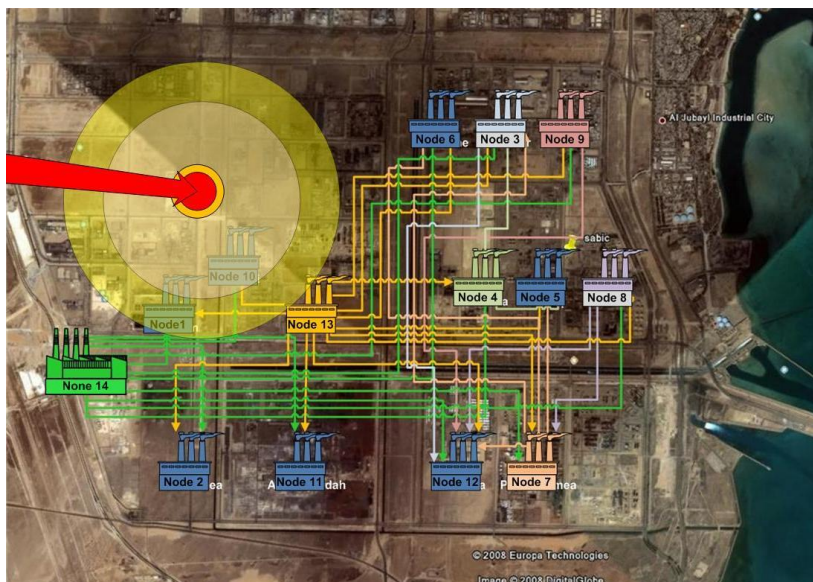


Figure 4-9 Scenario 2 location.

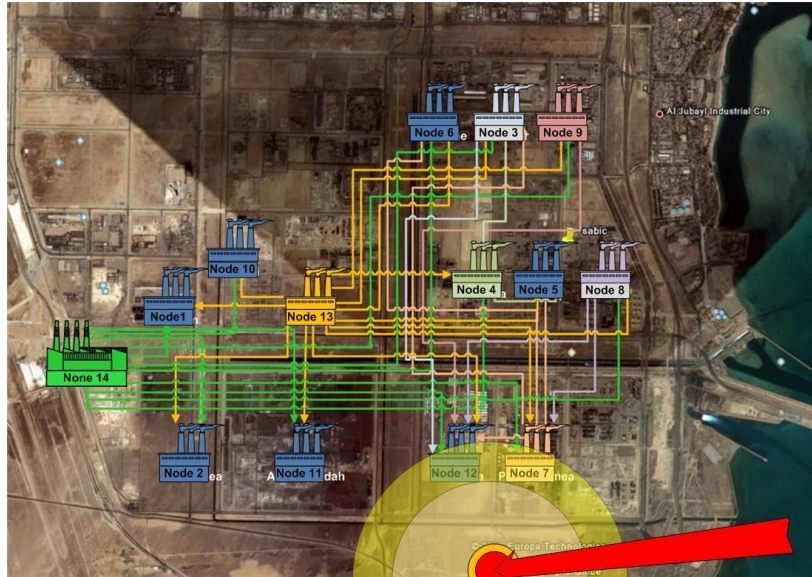


Figure 4-10 Scenario 3 location.

#### 4.5.2.1.2 Machine failure scenarios

Table 4-20 shows the details of the machine failure scenarios. These types of scenarios might happen to node and/or links. Also, the affected nodes are considered based on the PMCS cut sets.

Scenario	Type	Target Node	Effected Node
1	Minor	e17	Node3, Node5, Node6, Node7, Node12
2	Moderate	Node 4 and e2	Node3, Node4, Node5, Node 12
3	Major	Node 3 and Node 9	Node3, Node9, Node12

Table 4-19 Machine failure scenarios

Figure 4-11, Figure 4-12 and Figure 4-13 show these scenarios.

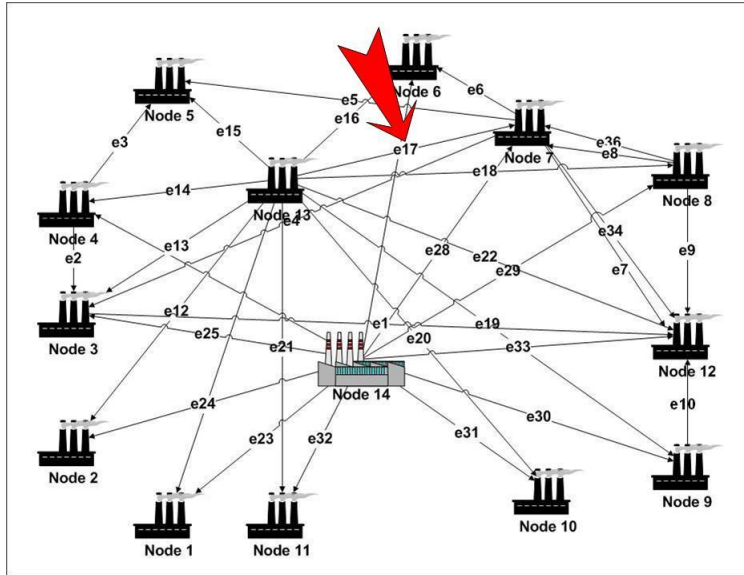


Figure 4-11 Machine failure, scenario 1, location.

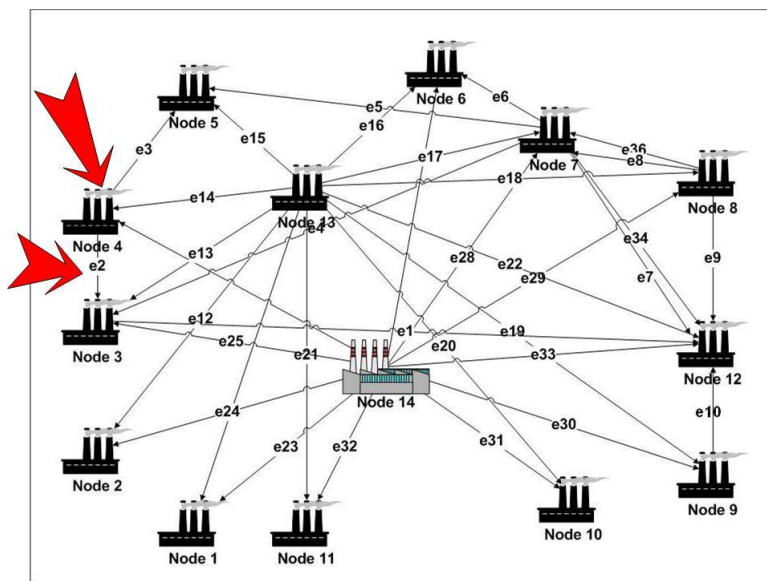


Figure 4-12 Machine failure, scenario 2, location.

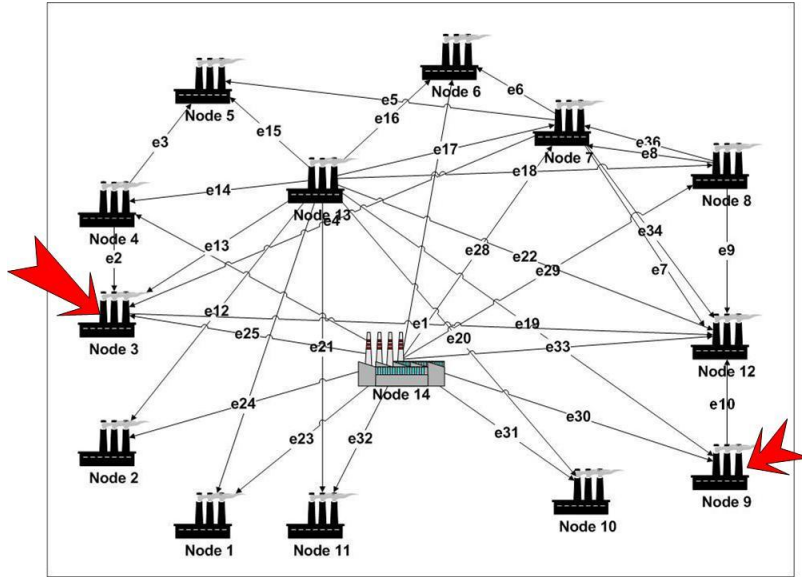


Figure 4-13 Machine failure, scenario 3, location.

#### 4.6 Performance Index (PI) calculation for PMCS for machine failure and terrorist attack scenarios

After completing the framework for the analysis of the infrastructures, we proceed to evaluate the PI for each node at JIC. The constructed scales are used to determine the level representative of the damage and impact. For example, looking at the constructed scale for economic impact on own property, Table 4-16, for node 3, we classified the impact from the the machine failure in scenario 1 as Level 2, hundreds of thousands of Saudi Riyals. Therefore, if there is a machine failure at node 3, the contribution to the PI for node 3, from the interruption of economic impact on own property would be the global weight of the PM (0.2388) multiplied by the assessed disutility (0.1311), which is 0.0313.

The remaining constructed scales are used to determine the contribution from the other PMs to the PI for node 3. When the summation across all the PMs is completed, the



resulting PI for node 3 in the scenario 1 machine failure is 0.0425. Once the assessment was completed for node 3, we analyzed the other nodes by following the same process. This process will be applied for all the scenarios in both machine failure and terrorist attacks. Once the PI is calculated for each node at JIC, the PI of each PMCS is calculated [10] as follows:

$$PI_k = \sum_i pmcs_k^i PI_i \quad (6)$$

Where:

- $PI_k$  is the performance index for *PMCS k*;
- $PMCS_k^i$  is a Boolean operator equal to unity when the PMCS k impacts the node *i*, and zero otherwise;
- $PI_i$  is the performance index for node *i* at JIC;
- *i* is the node at JIC (1–14);

For example, PMCS (node 3) impacts service to node 3 and node 12. The Boolean operator,  $PMCS_k^i$  for *k* representing the PMCS (node 3), equals unity when *i* equals 1 for node 3 and node 12, and zero in the remaining 12 nodes. The  $PI_k$  equals the *PI* for node 3 (0.0425) plus the *PI* for node 12 (0.0425), which is 0.085023. This process is repeated for every PMCS using Microsoft Excel. All the PIs for all PMCS in both machine failure scenarios and terrorist attack scenarios are shown in Appendix E.

After establishing the PI value of each PMCS, we start ranking them based on their PIs. The high PI is the more critical element at JIC. Table 4-20 shows PMCS ranked according to their PIs. The highest IP have extreme value where lower IP has very low value. These values are combined with susceptibility to determine the final vulnerability category (Table 3-6).

PI	PMCS	Value
0.4341	Node13	Extreme
0.3692	Node7, Node8, Node14, e8, e17, e18, e28, e29, e36,	
0.1275	Node4, e14, e26,	Very High
0.108	Node6, e6, e16, e27,	High
0.085	Node3, e2, e4, e13, e25,	Moderate
0.0425	Node9, Node12, e1, e3, e5, e10, e15, e19, e22, e30, e33, e34, e35,	Low
0	Node1, Node2, Node5, Node10, Node11, e7, e9, e11, e12, e20, e21, e23, e24, e31, e32,	Very Low

Table 4-20 PMCS ranked according to their values for scenario of in machine failure.

## 4.7 Results and Analysis

Section 3.2.4 provides guidance regarding the assessment of susceptibility. The final step is to develop the vulnerability list. This process involves an evaluation of the impact of each PMCS and assessing the susceptibility of its elements to machine failure or terrorist attacks. For example, looking at a PMCS with a relatively high PI, node 13 (Table 4-20), we find that it provides all JIC plants with gas. Failure of this node would result in disruption to all JIC plants. Since node 13 has one raw material, air, it has low probability to have a failure. As a result, we classified the susceptibility of node 13 as very low. We therefore place node 13 in the blue vulnerability category, (Table 3-6). We applied this process on the value tree of each decision maker for the six scenarios for both machine failures and terrorist attacks. After that, we aggregate vulnerability categorizations for all elements at JIC for each scenario as shown in Figure 4-14, Figure 4-15, Figure 4-16 and Figure 4-17.

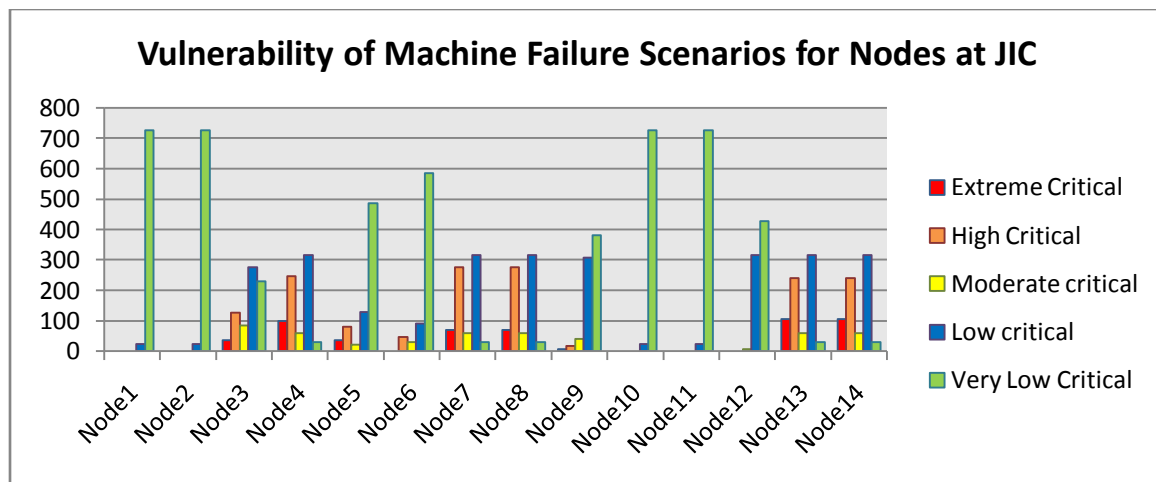


Figure 4-14 Vulnerability of Machine Failure Scenarios for Nodes at JIC.

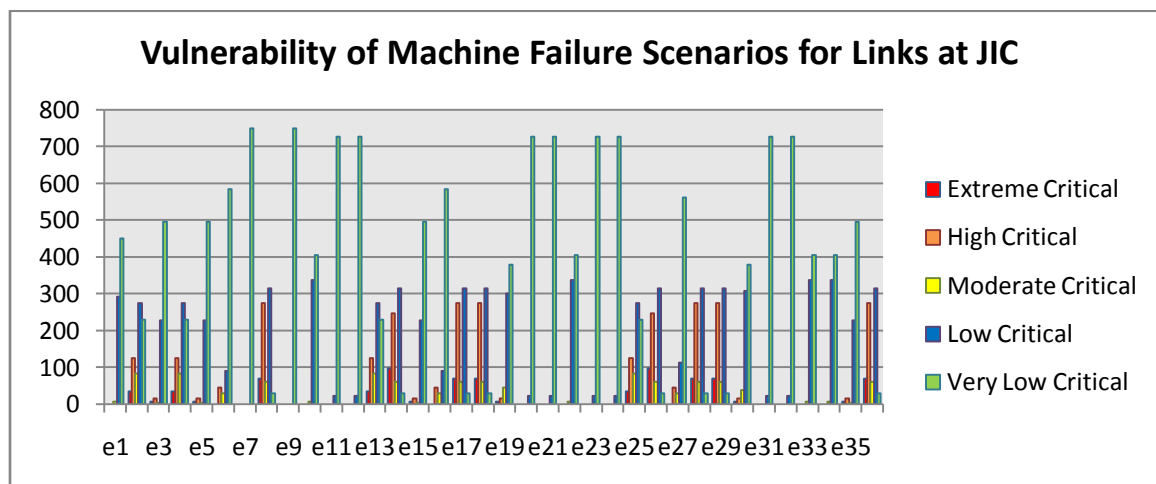


Figure 4-15 Vulnerability of Machine Failure Scenarios for Links at JIC.

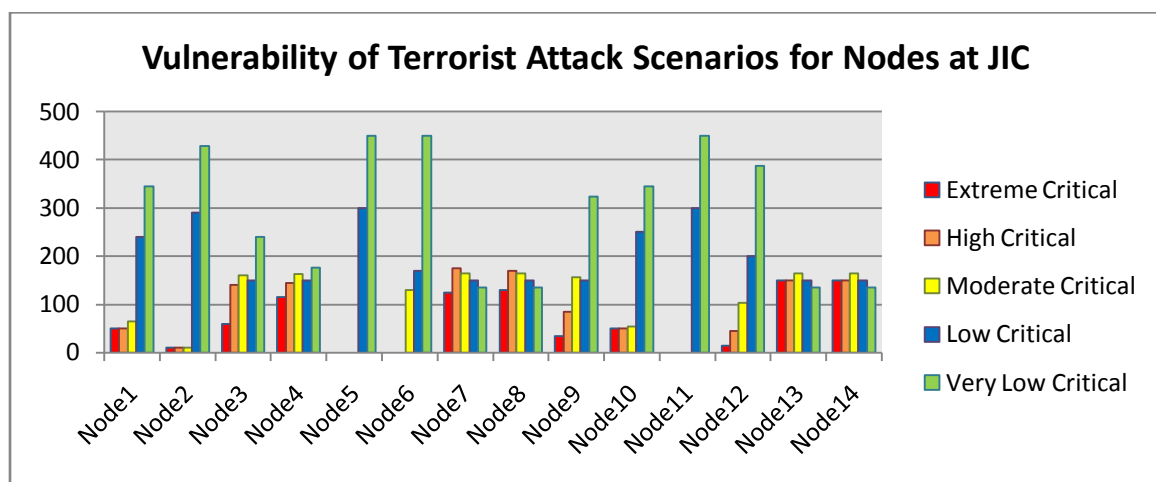


Figure 4-16 Vulnerability of Terrorist Attack Scenarios for Nodes at JIC

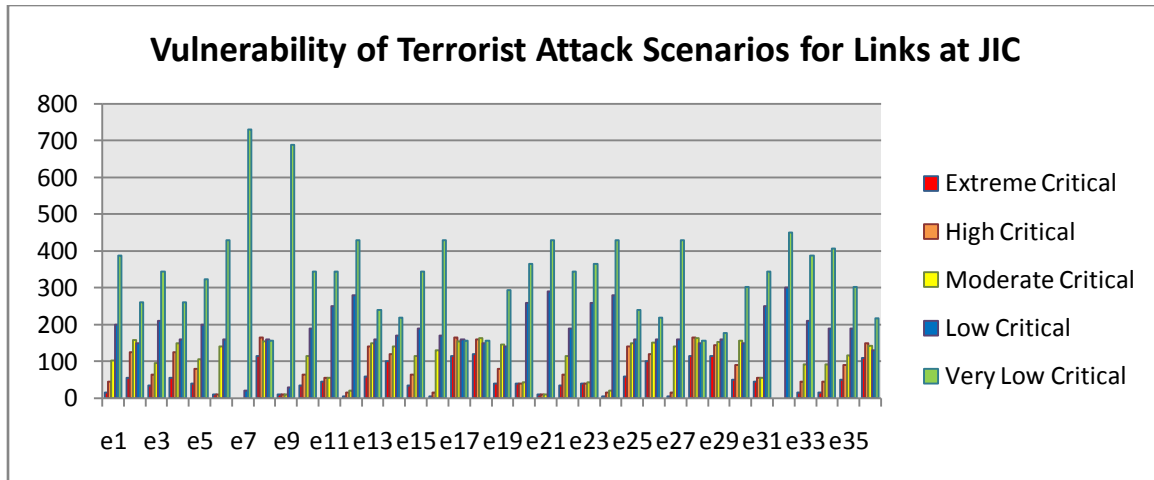


Figure 4-17 Vulnerability of Terrorist Attack Scenarios for Links at JIC

The previous results show the criticality for all elements at JIC. A graphical representation of the vulnerabilities of JIC elements to both machine failure and terrorist attack are shown in Figure 4-18 and Figure 4-19.

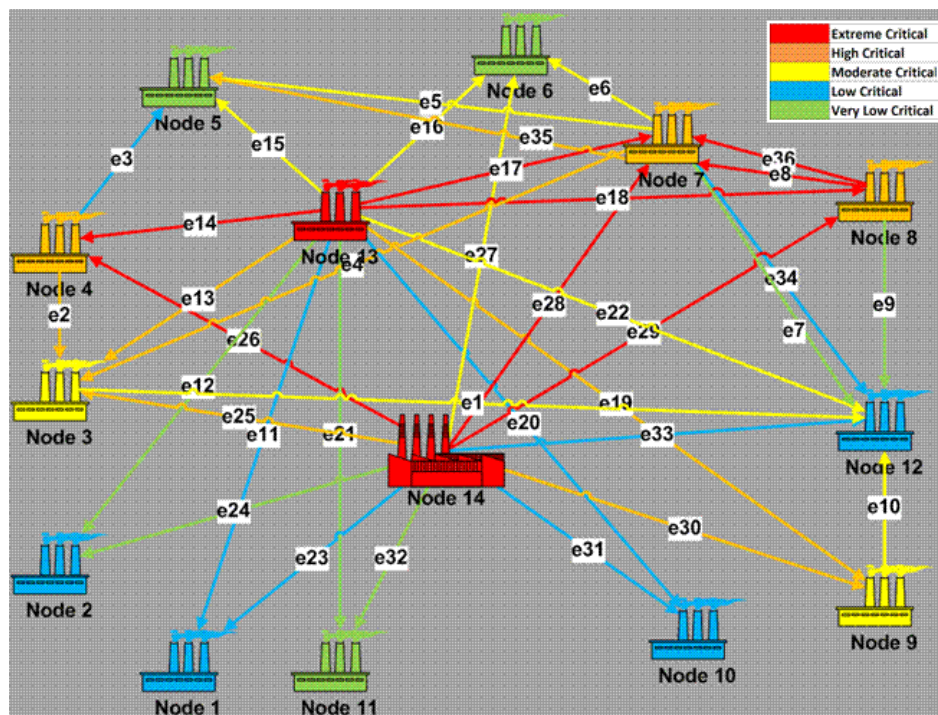


Figure 4-18 Graphical representation of the vulnerabilities of JIC to mechanical failure.

It is clear that several nodes are extreme critical in both type of scenarios. Node 13 and 14 are the most critical nodes because they are the oil and gas provider for all JIC plants. Also node 4, 7 and 8 are critical due to physical interdependencies of all other plants at JIC on their output. However links e8, e14, e17, e26, e28, e29 and e36 represent the most critical pipes at JIC. On the other hand, the criticality for node 1, 2, 6 and 11 are very low because they are edge nodes. Providing this result to the decision makers will help them to reduce the overall risk.

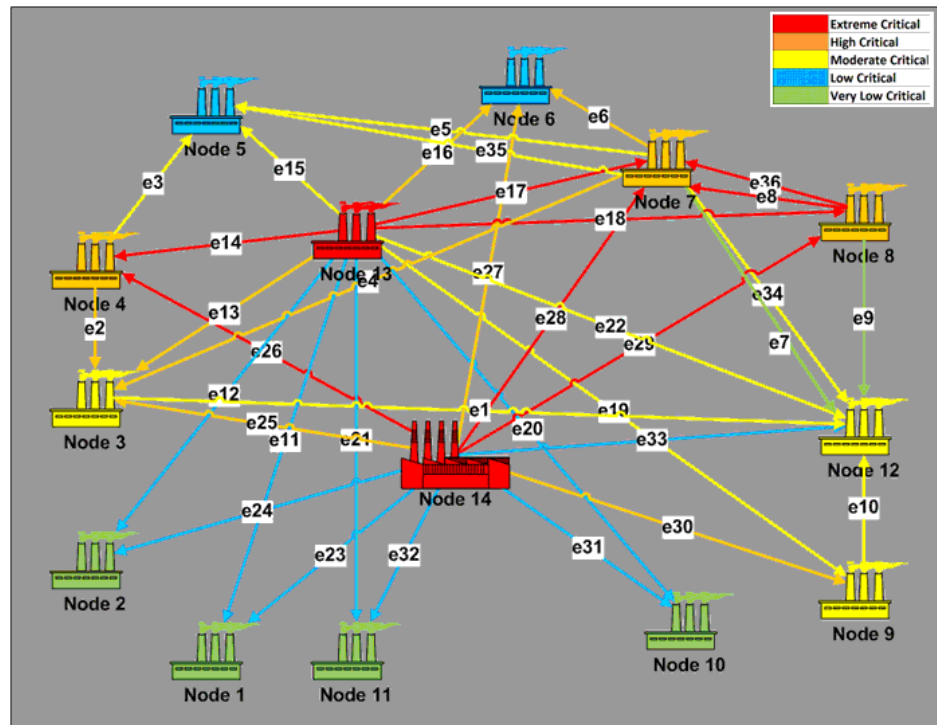


Figure 4-19 Graphical representation of the vulnerabilities of JIC to terrorist attack.

#### 4.8 Application of LPLC to Terrorist Attacks

Providing the decision makers only critical nodes and links could do not help them to realize how critical these elements. As it mentioned in section 3.3, we proposed an

approach to evaluate the nodes' criticality based on cost of loss. This approach is based on the location of nodes and how far it is from the attack. It takes into account the PMCS where node might located at zone 5 but it affected by a node located at zone 2 due to physical interdependence, part if PMCS. Figure 4-20, Figure 4-21 and Figure 4-22 show three terrorist attack scenarios where LPCL zones are applied. A MTTR is calculated for each node based on its location within LPCL zones.

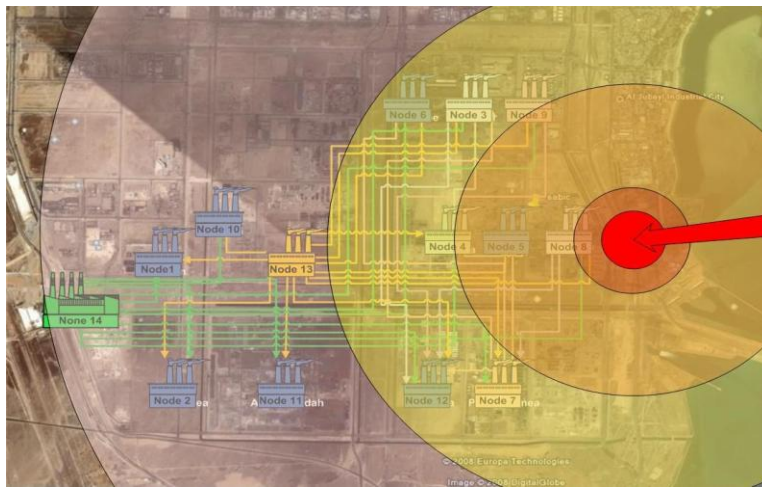


Figure 4-20 Scenario 1 with LPLC zones.

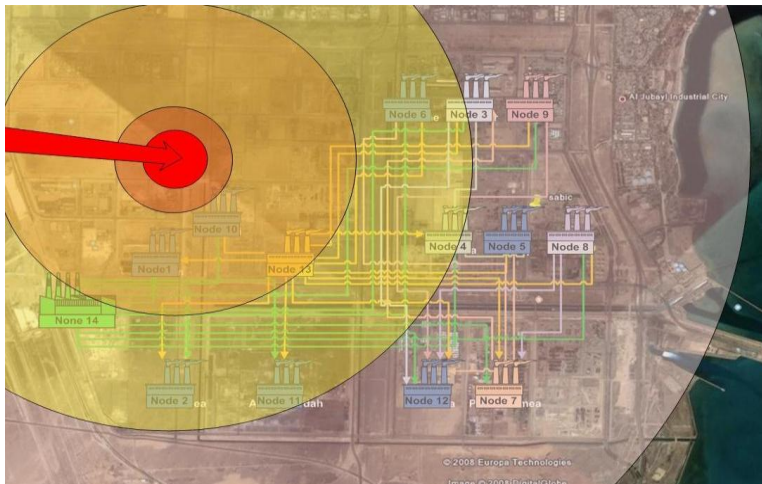


Figure 4-21 Scenario 2 with LPLC zones.

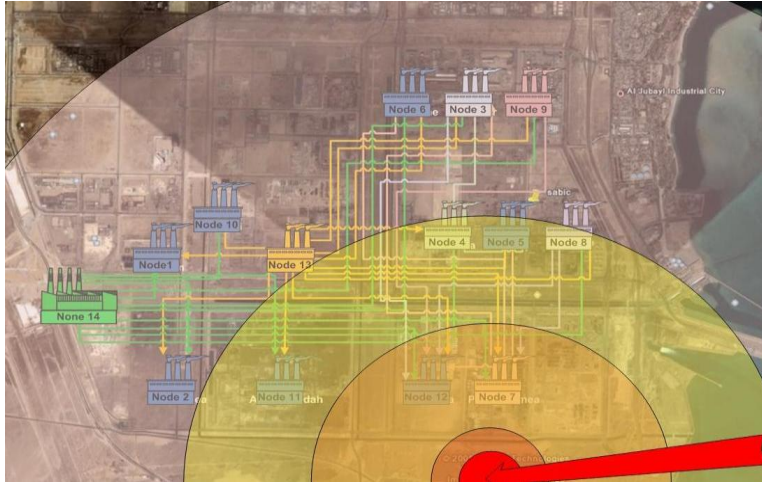


Figure 4-22 Scenario 3 with LPLC zones.

The cost of production is calculated as the final product of each plant. Prices of petrochemical in April 2009 are used to calculate the loss of each plant, (see Appendix F). Table 4-21, Table 4-22 and Table 4-23 show the loss for each node based on its location due to three terrorist attacks. In Table 4-21, node 8 is located in zone 2 so that its MTTR is 720 hours. Node 3, 5, 6, 7 and 12 are located in zone 3 and 4 but they have MTTR, 720 hours, equal to the MTTR of node 8. This is because node 8 is a cut set, physical dependence, for all these nodes and any interruption at node 8 will affect them.

Node Name	Zone	Risk Value	MTTR (h)	Affected Nodes	Product	Ton\hour	Price (SAR)	Loss in SAR	Total Loss in Riyals
Node 8	2	10%	720	3, 5, 6, 7, 12	Ethylene	114	2663	218,857,500	253,998,000
			720		Sodium Hydroxide	11	1500	12,330,000	
			720		Ethylene Dichloride	23	1388	22,810,500	
Node 5	3	30%	720	-	Polyethylene	86	4275	263,553,750	510,153,750
			720		Ethylene Glycol	171	2000	246,600,000	
Node 3	4	50%	720	12	MTBE	73	2250	118,327,500	645,435,000
			720		Polypropylene	171	4275	527,107,500	
Node 6	4	50%	720	-	Ammonia	53	1013	38,272,500	188,775,000
			720		Ethyl hexanol	20	4275	60,277,500	
			720		Urea	79	1050	59,850,000	
			720		Di-Octyl Phthalate(DOP)	6	6750	30,375,000	
Node 7	4	50%	720	3, 5, 6, 7	ethylene	228	2663	437,635,125	1,162,966,125
			720		Propylene	114	3225	265,095,000	
			720		Butene	228	2800	460,236,000	
Node 12	4	50%	720	-	ethylene	80	2663	153,200,250	212,396,400
			720		Propylene	9	3225	19,833,750	
			720		LLDPE	103	420	31,071,600	
			720		LDPE	27	420	8,290,800	
Node 4	3	30%	168	3, 5	Menthol	109	863	15,860,513	58,369,763
		30%	168		MTBE	112	2250	42,509,250	
Node 9	4	50%	72	12	fertilizer	542	900	35,100,000	35,100,000
Node 1	5	100%	12	-	Methanol	114	863	1,181,625	1,681,313
			12		Butanediol	9	4875	499,688	
Node 2	5	100%	12	-	Polypropylene	51	4275	2,635,538	2,635,538
Node 10	5	100%	12	-	Methanol	375	863	3,881,250	3,881,250
Node 11	5	100%	12	-	ethylene	154	2663	4,924,294	8,211,294
			12		Monoethylene Glycol	66	2000	1,575,000	
			12		Diethylene Glycol	71	2000	1,712,000	
									3,083,603,431

Table 4-21 Loss calculation due to scenario 1.



Node Name	Zone	Risk Value	MTTR	Affected Nodes	Product	Ton\Hour	Price	Loss in SAR	Total Loss in Riyals
Node 1	3	30%	168	-	Methanol	114	863	16,542,750	23,538,375
			168		Butanediol	9	4875	6,995,625	
Node 10	3	30%	168	-	Methanol	375	863	54,337,500	54,337,500
Node 2	4	50%	72	-	Polypropylene	51	4275	15,813,225	15,813,225
Node 11	4	50%	72	-	ethylene	154	2663	29,545,763	49,267,763
			72		Monoethylene Glycol	66	2000	9,450,000	
			72		Diethylene Glycol	71	2000	10,272,000	
Node 6	4	50%	72	-	Ammonia	53	1013	3,827,250	18,877,500
			72		Ethyl hexanol	20	4275	6,027,750	
			72		Urea	79	1050	5,985,000	
			72		Di-Octyl Phthalate(DOP)	6	6750	3,037,500	
Node 4	4	50%	72	3, 5, 12	Menthol	109	863	6,797,363	25,015,613
			72		MTBE	112	2250	18,218,250	
Node 3	5	100%	72	12	MTBE	73	2250	11,832,750	64,543,500
			72		Polypropylene	171	4275	52,710,750	
Node 5	5	100%	72	-	Polyethylene	86	4275	26,355,375	51,015,375
			72		Ethylene Glycol	171	2000	24,660,000	
Node 12	5	100%	72	-	ethylene	80	2663	15,320,025	20,548,740
			72		Propylene	9	3225	1,983,375	
			72		LLDPE	103	420	3,107,160	
			12		LDPE	27	420	138,180	
Node 7	5	100%	12	3, 5, 6, 7	ethylene	228	2663	7,293,919	19,382,769
			12		Propylene	114	3225	4,418,250	
			12		Butene	228	2800	7,670,600	
Node 8	5	100%	12	3, 5, 6, 7, 12	ethylene	114	2663	3,647,625	4,233,300
			12		Sodium Hydroxide	11	1500	205,500	
			12		Ethylene Dichloride	23	1388	380,175	
Node 9	5	100%	12	12	fertilizer	542	900	5,850,000	5,850,000
									352,423,659

Table 4-22 Loss calculation due to scenario 2.

Node Name	Zone	Risk Value	Hours	Affected Nodes	Product	Ton\Hour	Price	Loss in SAR	
Node 7	3	30%	168	3, 5, 6, 12	ethylene	228	2663	102,114,863	271,358,763
			168		Propylene	114	3225	61,855,500	
			168		Butene	228	2800	107,388,400	
Node 12	3	30%	168	-	ethylene	80	2663	35,746,725	49,559,160
			168		Propylene	9	3225	4,627,875	
			168		LLDPE	103	420	7,250,040	
			168		LDPE	27	420	1,934,520	
Node 5	4	50%	168		Polyethylene	86	4275	61,495,875	119,035,875
			168		Ethylene Glycol	171	2000	57,540,000	
Node 6	5	100%	168	-	Ammonia	53	1013	8,930,250	44,047,500
			168		Ethyl hexanol	20	4275	14,064,750	
			168		Urea	79	1050	13,965,000	
			168		Di-Octyl Phthalate(DOP)	6	6750	7,087,500	
Node 3	5	100%	168	12	MTBE	73	2250	27,609,750	150,601,500
			168		Polypropylene	171	4275	122,991,750	
Node 4	4	50%	72	3, 5, 12	Menthol	109	863	6,797,363	25,015,613
			72		MTBE	112	2250	18,218,250	
Node 8	4	50%	72	3, 5, 6, 7, 12	ethylene	114	2663	21,885,750	25,399,800
			72		Sodium Hydroxide	11	1500	1,233,000	
			72		Ethylene Dichloride	23	1388	2,281,050	
Node 11	4	50%	72	-	ethylene	154	2663	29,545,763	49,267,763
			72		Monoethylene Glycol	66	2000	9,450,000	
			72		Diethylene Glycol	71	2000	10,272,000	
Node 1	5	100%	12	-	Methanol	114	863	1,181,625	1,681,313
			12		Butanediol	9	4875	499,688	
Node 2	5	100%	12	-	Polypropylene	51	4275	2,635,538	2,635,538
Node 9	5	100%	12	12	fertilizer	542	900	5,850,000	5,850,000
Node 10	5	100%	12	-	Methanol	375	863	3,881,250	3,881,250
									748,334,073

Table 4-23 Loss calculation due to scenario 3.

## 4.9 Resources Allocation to Reduce the Overall Risk

After identifying and prioritizing all the critical locations at CI. Decision maker needs to know what is the best way to allocate a available resources to protect CI against damage. In this Thesis we proposed a new method to allocate resources which is based on reducing the worst damage that can occur or reduce expected damages. This method divides all elements at CI are divided according to their criticality. Then empirical values are used to disrepute the resources all resources.

Very Low Critical	Low Critical	Moderate Critical	High Critical	Extreme Critical	Criticality
5%	10%	20%	25%	40%	Allocated Resources

Table 4-24 Resource Allocation Table

Table 4-24 shows the amount of recourses that will be allocated to harden the critical elements. The criticality is explained in Section 4.7. Figure 4.18 and Figure 4-19 show the critical elements in both machine failure and terrorist attack failure scenarios respectively. That means that the extreme critical elements will get 40% of the available resources for protection while very low critical elements will receive only 5%. For example, the allocation of SAR 5,000,000 to protect JIC elements against terrorist attack will assign SAR 2,000,000, 40% of the total amount, to protect nodes 13 and 14 which are the extreme critical node in Figure 4-19. Table 4-25 shows how to allocate SAR 5,000,000 to reduce the overall risk of all JIC's nodes.

Very Low Critical	Low Critical	Moderate Critical	High Critical	Extreme Critical	Criticality
5%	10%	20%	25%	40%	100%
4	2	3	3	2	No. of Nodes
Allocating SAR 5,000,000 to reduce the overall risk					
250,000	500,000	1,000,000	1,250,000	2,000,000	Money allocated
62,500	250,000	333,333	416,667	1,000,000	Money allocated per Node

Table 4-25 Example of resource allocation method

## **Chapter Five: Conclusion**

### **5.1 Conclusion**

In this Thesis, we discussed a methodology for identifying the *critical locations* in petrochemical industry. This methodology can identify individual critical locations and combinations of locations, which when attacked through simultaneous or sequential events could lead to significant consequences. All the critical locations are ranked according to their potential impact which will be used as the basis of risk informed decision making. The PMCS technique is proposed in this thesis as new technique to be applicable for homogenous and heterogeneous networks. A new approach, LPLC, was presented to provide a ranking mechanism to classify all CIs according to the impacting total loss cost.

This methodology is applied to the petrochemical industries at JIC in Saudi Arabia. All the JIC elements are ranked according to their criticality. Six scenarios are tested. Both machine failure and terrorist attack are examined in this thesis.

### **5.2 Future Work**

This approach could be applied for other types of CIs e.g. oil pipeline, water-supply network and power grid network. Also, applying cascade failure that caused by one CI and deployed to the other CIs. This work does not take link capacity into account so that it would be helpful to include the concept of Input Output Model (IOM).

## Bibliography

- [1] K. R. Al-Rodhan, "The Impact of the Abqaiq Attack on Saudi Energy Security," The Center for Strategic and International Studies Saudi-U.S. Relations Information Service, 2006.
- [2] G. E. Apostolakis and D. M. Lemon, "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism," *Risk Analysis*, vol. 25, no. 2, pp. 361-376, Apr. 2005.
- [3] George Mason University School of Law, "Canada's Approach to Critical Infrastructure Protection," *The CIP Report*, vol. 5, no. 12, p. 3, Jun. 2007.
- [4] wikipedia. (2009, Jan.) Probability. [Online]. <http://en.wikipedia.org/wiki/Probability>
- [5] J. Stephenson, "Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed," The Library of Congress, Washington, D.C., GAO Report to Congress, 2005.
- [6] J. B. Stephenson, "Federal Action Needed to Address Security Challenges at Chemical Facilities," The Library of Congress, Washington, D.C., GAO Report to Congress, 2004.
- [7] H. O. Rosel, "Protecting Our Waters Within: A Vulnerability Assessment of Maritime Infrastructure Within Coast Guard Sector Ohio Valley," Naval Postgraduate School, 2006.
- [8] S. Rinaldi, T. Kelly, and J. Peerenboom, "Complexities in Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 1, pp. 11-25, Jan. 2001.
- [9] Reuters. (2008, Jun.) Gulf petchem boom faces cost, labour challenges. [Online]. <http://uk.reuters.com/articlePrint?articleId=UKL20582920080120>
- [10] R. Popp, T. Armour, T. Senator, and K. Nymrych, "Countering terrorism through information technology," *Communications of the ACM*, vol. 47, no. 3, pp. 36-43, Mar. 2004.
- [11] D. Pennington, "Chemical Facility Preparedness: A comprehensive Approach," Master Thesis, Naval Postgraduate School, Monterey, CA, 2006.
- [12] OHS, "National Strategy for Homeland Security," U.S. Executive Office of the President, 2002.
- [13] E. Luijff and M. Klaver, "Protecting a Nation's Critical Infrastructure: The First Steps," in *IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, 2004.

- [14] T. G. Lewis, *Critical Infrastructure Protection in Homeland Security (Defending a Networked Nation)*. New Jersey, USA: John Wiley&Sons, 2006.
- [15] M. Lauzon. (2008, Jun.) Petrochemical Industry. [Online].  
<http://www.thecanadianencyclopedia.com/index.cfm?PgNm=TCE&Params=A1ARTA0006251>
- [16] J. Kouri. (2005, May) Preventing Terrorist Attacks at Chemical Facilities. [Online].  
<http://mensnewsdaily.com/2005/05/06/preventing-terrorist-attacks-at-chemical-facilities/>
- [17] D. M. Kirschbaum. (2003) Calculated Risk. [Online].  
<http://nonprofitrisk.org/library/articles/risk01002000.shtml>
- [18] M. Heller, "Interdependencies in Civil Infrastructure Systems," *The Bridge*, vol. 31, no. 4, pp. 9-14, 2001.
- [19] Y. Haimes and T. Longstaff, "The Role of Risk Analysis in the Protection of Critical Infrastructures against Terrorism," *Risk Analysis*, vol. 22, no. 2002, pp. 439-444, Jun. 2002.
- [20] GOIC. (2007, Nov.) GCC Petrochemical Industry. [Online].  
<http://www.goic.org.qa/GOICinthenews.html>
- [21] C. Doyle, "Terrorism Legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001," Library of Congress Government RS21051, 2002.
- [22] C. Dickey, "Saudi Storms," *Newsweek*, Oct. 2005, <http://www.newsweek.com/id/50917>.
- [23] A. H. Cordesman and K. R. Al-Rodhan, "The Gulf Military Forces in an Era of Asymmetric War: Saudi Arabia," Center for Strategic and International Studies, 2006.
- [24] A. H. Cordesman and N. Obaid, "Saudi Petroleum Security: Challenges and Responses," Center for Strategic and International Studies, 2004.
- [25] F. J. Cilluffo, "Preventing Terrorist Attacks on America's Chemical Plants," House Committee on Homeland Security Serial No. 109–20, 2005.
- [26] J. J. Carafano, "Principles for Congressional Action on Chemical Security," 2006.
- [27] B. Bongar, L. M. Brown, L. E. Beutler, J. N. Breckenridge, and P. G. Zimbardo, *Psychology of Terrorism*. New York: Oxford University Press, 2006.
- [28] R. E. Bollinger, D. G. Clark, A. M. Dowell III, R. M. Ewbank, D. C. Hendershot, W. K. Lutz, S. I. Meszaros, D. E. Park and E. D. Wixom, "Inherently Safer Chemical Processes: a Life Cycle

Approach," Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.

- [29] R. Abbas, "The Threat of Public Data Availability on Critical Infrastructure Protection (CIP), and the Level of Awareness Amongst Security Experts in Australia," Master Thesis, University of Wollongong, 2006.
- [30] US General Accounting Office, "Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown," The Library of Congress Homeland Security GAO-03-439, 2003.
- [31] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," 2004.
- [32] Department of Transportation. (2005) Risk Management Definitions. [Online].  
<http://www.phmsa.dot.gov/portal/site/PHMSA/menuitem.ebdc7a8a7e39f2e55cf2031050248a0c/?vgnextoid=36d8a73ff3d0d110VgnVCM1000009ed07898RCRD&vgnnextchannel=5ea0c0124500d110VgnVCM1000009ed07898RCRD&vgnnextfmt=print>
- [33] British Standards Institute, "Risk management - Vocabulary - Guidelines for use in standards," ISO/IEC Guide 73:2002, 2002.
- [34] Office of Hazardous Materials Safety. (2008) Risk Management. [Online].  
<http://www.phmsa.dot.gov/portal/site/PHMSA/menuitem.ebdc7a8a7e39f2e55cf2031050248a0c/?vgnextoid=36d8a73ff3d0d110VgnVCM1000009ed07898RCRD&vgnnextchannel=5ea0c0124500d110VgnVCM1000009ed07898RCRD&vgnnextfmt=print>
- [35] American Chemistry Council. (2008, Jun.) Did You Know. [Online].  
[http://www.americanchemistry.com/s\\_acc/sec\\_didyouknow.asp?CID=198&DID=524](http://www.americanchemistry.com/s_acc/sec_didyouknow.asp?CID=198&DID=524)
- [36] S. Parongama, B. Kinjal, and B. Turbasu, "Phase transitions in a network with a range dependent connection probability," *American Physical Society*, vol. 66, no. 3, pp. 0371021-0371024, 2002.
- [37] S. Ritter and J. Weber, "Critical Infrastructure Protection: Survey of worldwide Activities," in *Critical Infrastructure Protection (CIP) Workshop*, Frankfurt, 2003.
- [38] T. Tagarev and P. Nickolay, "Planning Measures and Capabilities for Protection of Critical Infrastructures," *Information & Security Journal*, vol. 22, pp. 38-48, 2007.
- [39] J. Min, W. Beyeler, T. Brown, Y. Son, and A. Jones, "Toward modeling and simulation of critical national infrastructure interdependencies," *IIE TRANSACTIONS*, vol. 39, no. 1, pp. 57-71, Jan.



2007.

- [40] G. W. Bush, "The Department of Homeland Security," the White House, 2002.
- [41] H. Barry, "State Official's Guide to Critical Infrastructure Protection," The Council of State Governments, 2003.
- [42] U.S. Department of Homeland Security Strategic Plan, "One Team, One Mission, Securing Our Homeland," U.S. Department of Homeland Security, 2008.
- [43] Public Safety Canada. (2009, Jan.) Joint Infrastructure Interdependencies Research Program. [Online]. <http://www.publicsafety.gc.ca/prg/em/jiirp/index-eng.aspx>
- [44] CPNI. (2009, Jan.) Center for the Protection of National Infrastructure. [Online]. <http://www.cpni.gov.uk/aboutcpni188.aspx>
- [45] TISN. (2008, Oct.) Trusted Information Sharing Network for Critical Infrastructure Protection. [Online]. <http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/AbouttheTISN>AbouttheTISN>
- [46] Australian Government Attorney-General's Department. (2008, Oct.) Critical Infrastructure Protection. [Online]. [http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity\\_CriticalInfrastructureProtection](http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection)
- [47] Federal Office for Information Security (BSI). (2008, Oct.) Annual Report 2003. [Online]. <http://www.bsi.bund.de/english/publications/annualreport/BSI-AnnualReport2003.pdf>
- [48] H. Deguchi, *Economics as an Agent-Based Complex System*. New York, NY: Springer, 2004.
- [49] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann. (2006, Aug.) Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. [Online]. <http://www.inl.gov/technicalpublications/Documents/3489532.pdf>
- [50] A. Sage, *Methodology for Large-Scale Systems*. New York, NY: McGraw-Hill, 1977.
- [51] Y. Y. Haimes and P. Jiang, "Leontief-Based Model of Risk in Complex Interconnected Infrastructures," *Journal of Infrastructure Systems*, vol. 7, no. 1, pp. 1-12, 2001.
- [52] Y. Y. Haimes, et al., "Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology," *Journal of Infrastructure System*, vol. 11, pp. 67-79, 2005.

- [53] I. R. Santos and Y. Y. Haimes, "Applying the Partitioned Multiobjective Risk Method (PMRM) to Portfolio Selection," *Risk Analysis*, vol. 24, no. 3, pp. 697-713, 2004.
- [54] J. Martí, J. Hollman, C. Ventura, and J. Jatskevich, "Design for survival. Real-time infrastructures coordination," in *Proceedings of the International Workshop on Complex Network and Infrastructure Protection (CNIP2006)*, 2006.
- [55] J. Hollman, J. R. Marti, J. Jatskevich, and K. D. Sriva, "Dynamic islanding of critical infrastructures: a suitable strategy to survive and mitigate extreme events," *International Journal of Emergency Management (IJEM)*, vol. 4, no. 1, 2007.
- [56] A. L. Barabasi, *Linked: The New Science of Networks*. Cambridge, MA: Perseus, 2002.
- [57] L. Buzna, K. Peters, and D. Helbing, "Modelling the Dynamics of Disaster Spreading in Networks," *Physica A: Statistical Mechanics and its Applications*, vol. 363, no. 1, pp. 132-140, 2006.
- [58] R. Albert, H. Jeong, and A. L. Barabasi, "Error and Attack Tolerance of Complex Networks," *Nature*, vol. 406, pp. 378-381, 2000.
- [59] R. Zimmerman and C. E. Restrepo, "The Next Step: Quantifying Infrastructure Interdependencies to Improve Security," *International Journal of Critical Infrastructures*, vol. 2, no. 2/3, pp. 215-230, 2006.
- [60] K. L. Stamber, N. S. Brodsky, and R. J. Detry, "Fast Turnaround Analysis of Critical Infrastructure and Tool Development to Support Analytic Efforts," in *Proceedings of Working Together: R&D Partnerships in Homeland Security*, 2005.
- [61] National Infrastructure Institute. (2009, Jan.) Target Analysis. [Online]. <http://www.ni2cie.org/targetanalysis.php.htm>
- [62] R. Abdalla, V. Tao, and H. Ali, "Location-Based Infrastructure Interdependency: New Tenn, New Modeling Approach," in *Proceedings of Geoinformatics*, 2005.
- [63] P. F. Deisler, "A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism," *Risk Analysis*, vol. 22, no. 3, pp. 405-413, Jun. 2002.
- [64] B. J. Garrick, "Perspectives on the Use of Risk Assessment to Address Terrorism," *Risk Analysis*, vol. 22, no. 3, pp. 421-423, Jul. 2002.
- [65] G. E. Apostolakis, "How Useful is Quantitative Risk Assessment," *Risk Analysis*, vol. 24, no. 3, pp. 515-520, Jun. 2004.

- [66] S. Kaplan and B. J. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, vol. 1, no. 1, pp. 11-27, 1981.
- [67] B. J. Garrick, J. E. Hall, J. C. McDonald, T. O'Toole, P. S. Probst, E. R. Parker, R. Rosenthal, A. W. Trivelpiece, L. A. Van Arsdales and E. L. Zebroski, "Confronting the Risks of Terrorism: Making the Right Decisions," *Reliability Engineering and System Safety*, vol. 86, no. 2, pp. 129-176, Nov. 2004.
- [68] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*. New York: American Elsevier Publishing Company, 1980.
- [69] B. C. Ezell, J. V. Farr, and I. Wiese, "Infrastructure Risk analysis Model," *Journal of Infrastructure Systems*, vol. 6, no. 3, pp. 114-117, Sep. 2000.
- [70] G. Ballocco, A. Carpignano, and M. Argiulo, "Merging Cut Sets and Reliability Indexes for Reliability and Availability of Highly Meshed Networks," in *European Safety and Reliability Conference (ESREL)*, Maastricht, Belgium, 2003.
- [71] R. Weil and G. E. Apostolakis, "A methodology for the Prioritization of Operating Experience in Nuclear Power Plants," *Reliability Engineering and System Safety*, vol. 74, no. 1, pp. 23-42, Oct. 2001.
- [72] R. Gregory and R. L. Keeney, "Creating Policy Alternatives Using Stakeholder Values," *Management Science*, Vol. 40, No. 8, pp.1035-1048, 1994., vol. 40, no. 8, pp. 1035-1048, Aug. 1994.
- [73] R. T. Clemen, *Making Hard Decisions: An Introduction to Decision Analysis*, 2nd ed. Belmont, CA: Duxbury Press, 1996.
- [74] T. L. Saaty, *The Analytic Hierarchy Process: Planning, Priority Setting, and Resource Allocation*. New York: McGraw-Hill, 1980.
- [75] N. S. Grigg, "Water Utility Security: Multiple Hazards and Multiple Barriers," *Journal of Infrastructure Systems*, vol. 9, no. 2, pp. 81-88, Jun. 2003.
- [76] W. R. Hughes, "Deriving Utilities Using the Analytic Hierarchy Process," *Socio- Economic Planning Sciences*, vol. 20, no. 6, pp. 393-395, 1986.
- [77] R. J. Budnitz, et al., "Use of technical expert panels: Applications to probabilistic seismic hazard analysis," *Risk Analysis*, vol. 18, 1998.
- [78] S.A.Patterson and G.E. Apostolakis, "Identification of Critical Locations across Multiple

Infrastructures for Terrorist Actions," *Reliability Engineering and System Safety*, vol. 92, pp. 1183-1203, 2007.

- [79] D. Michaud and G. E. Apostolakis, "A Methodology for Ranking the Elements of Water-Supply Networks," *Journal of Infrastructure Systems*, vol. 12, pp. 230-242, 2006.
- [80] A. M. Koonce, G. E. Apostolakis, and B. K. Cook, "Bulk power risk analysis: Ranking infrastructure elements according to their risk significance," *International Journal of Electrical Power & Energy Systems*, vol. 30, no. 3, pp. 169-183, Mar. 2008.
- [81] American Chemical Industry. (2008, Oct.) ACC Supports Federal Chemical Security Legislation. [Online].  
[http://www.americanchemistry.com/s\\_acc/sec\\_policyissues.asp?CID=329&DID=1156](http://www.americanchemistry.com/s_acc/sec_policyissues.asp?CID=329&DID=1156)
- [82] Saudi Arabian Monetary Agency (SAMA), "Forty-Fourth Annual Report," 2008.
- [83] Global, "Petrochemical Industry Saudi Arabia Economic and Strategic Outlook," Global Investment House, 2008.
- [84] wikipedia. (2008, Dec.) Jubail. [Online]. <http://en.wikipedia.org/wiki/Jubail>
- [85] Sabic. (2008, Dec.) Saudi Basic Industries Corporation. [Online].  
<http://www.sabic.com/asia/en/newsandmediarelations/news/20081119.aspx>
- [86] J. A. Bondy and U. S. Murty, *Graph Theory with Applications*. New York: North-Holland, 1980.
- [87] R. Accorsi, G. Apostolakis, and E. Zio, "Prioritizing stakeholder concerns in environmental risk management," *Journal of Risk Research*, vol. 2, p. 11-29, 1999.
- [88] NIPC, "Risk Management: As essential Guide to Protecting Critical Assets," National Infrastructure Protection Center, 2002.
- [89] H. Li, et al., "Ranking the Risks from Multiple Hazards in a Small Community," *Risk Analysis*, vol. 29, no. 3, pp. 438-456, 2009.
- [90] Y. Y. Haimes, "Roadmap for Modeling Risks of Terrorism to the Homeland," *JOURNAL OF INFRASTRUCTURE SYSTEMS*, vol. 8, no. 2, pp. 35-41, Jun. 2002.
- [91] G. G. Brown, W. Carlyle, K. Wood, and J. Salmeron, "Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses," Naval Postgraduate School, 2005.

## Appendix A

### Survey Instructions

- A. As a Decision Maker in a petrochemical organization/company, you are given a set of categories. In each category (i.e., Impact Category), there are many options (i.e., Economic vs. Image).
- B. You kindly requested to select one option among these two options (i.e., Image) which you believe it is more important to your petrochemical organization/company.
- C. For the selected (i.e., Image), give a scale from 1 to 9 to weight the importance of the selected over the other to your petrochemical organization/company.
- D. The scale values are selected according to what is shown below:
  - Scale = 1 for Equally Important Option
  - Scale = 3 for Weakly Important Option
  - Scale = 5 for Moderately Important
  - Scale = 7 Strongly Important
  - Scale = 9 Extremely Important

#### **Impact Categories:**

1. Economic vs. Image ( )
2. Economic vs. Health & Safety ( )
3. Image vs. Health & Safety ( )
4. Environment vs. Economic ( )
5. Environment vs. Health & Safety ( )
6. Environment vs. Image ( )

#### **Economics:**

1. External vs. Own ( )

#### **Image:**

1. Public vs. Customer ( )
2. Public vs. Workers ( )
3. Customers vs. Workers ( )

#### **Health & Safety:**

1. General Public vs. Workers ( )
2. Long-term Impact vs. Immediate Casualties ( )

### Help:

1. Impact on Health and Safety: Include both temporary and permanent impacts on Health and Safety.
2. Impact on Image: Internal Image within the Administration, Image with the General Public, Image with Critical Customers and Image with Individual Customers.
3. Impact on Economic: Includes Economic Impact on Own Property and Economic Impact on Other People's Property.
4. Impact on Environment: Include all the impacts on the Environment inside and outside the organization.
5. For the background specialization, kindly mention your professional specializations such as Engineering, Management, Economic/Finance, Security, etc.

### Example:

#### Impact Categories

1. Economic vs. Image ( \_\_3\_\_ ) → Image Impact is Weakly Important than Economic Impact
2. Economic vs. Health & Safety ( \_\_9\_\_ ) → Economic Impact is Extremely Important than Health&Safety Impact
3. Image vs. Health & Safety ( \_\_3\_\_ ) → Health&Safety Impact is Weakly Important than Image Impact
4. Environment vs. Economic ( \_\_9\_\_ ) → Economic Impact is Extremely Important than Environment Impact
5. Environment vs. Health & Safety ( \_\_1\_\_ ) → Health&Safety Impact is Equally Important than Environment Impact
6. Environment vs. Image ( \_\_7\_\_ ) → Image Impact is Strong

## Appendix B

Production Minimum Cut Set of petrochemical industry network at JIC:

Node1 = {Node 1, Node 13, Node 14, e11, e23};

Node2 = {Node 2, Node 13, Node 14, e12, e24};

Node3 = {Node 3, Node 4, Node 7, Node 8, , Node 13, Node 14, e2, e4, e8, e13, e14, e17, e18, e25, e26, e28, e29 ,36};

Node4 = {Node4, Node 13, Node 14, e14, e26};

Node5 = {Node 4, Node 5, Node 7, Node 8, Node 13, Node 14, e3, e5, e8, e14, e15, e17, e18, e26, e28, e29, e35, e36};

Node6 = {Node 6, Node 7, Node 8, Node 13, Node 14, e6, e8, e16, e17, e18, e27, e28, e29, e36};

Node7 = {Node 7, Node 8, Node 13, Node 14e, 8, e17, e18, e28, e29, e36};

Node8 = {Node8, Node 13, Node 14, e18, e29};

Node9 = {Node9, Node 13, Node 14, e19, e30};

Node10 = {Node10, Node 13, Node 14, e20, e31};

Node11 = {Node11, Node 13, Node 14e, 21, e32}

Node12= {Node 3, Node 4, Node 7, Node 8, Node 9, Node 12, Node 13, Node 14, e1, e2, e4, e8, e10, e13, e14, e17, e18, e19, e22, e25, e26, e28, e29, e30 e33, e34, e36}

Node 13 = {Node 13};

Node 14 = {Node 14}.

## Appendix C

### Data from Decision Maker 1 (DM1):

#### Performance Measures Weights Assessment

	Impact Categories			
	H&S	Image	Economics	Environment
H&S	1.00	5.0000	2.0000	3.0000
Image	0.20	1.00	0.1429	0.1111
Economics	0.50	7.00	1.00	3.0000
Environment	0.33	9.00	0.33	1.00
Weights	0.4291	0.0501	0.3184	0.2024

Consistency index	17.3809
Consistency ratio	19.3121

Performance Measures		
	Impact on Health and Safety	
	Workers	Public
Workers	1.00	7.00
Public	0.14	1.00
Weights	0.8750	0.1250

	Impact on Image		
	Internal	General Public	Customers
Internal	1.00	5.00	2.00
General Public	0.20	1.00	0.14
Customers	0.50	7.00	1.00
Weights	0.5364	0.0800	0.3836

Consistency index	7.8777
Consistency ratio	13.5823

	Impact on Economics	
	Own	External
Own	1.00	5.00



External	0.50	1.00
Weights	0.7500	0.2500

**Data from Decision Maker 2 (DM2):**

	Impact Categories			
	H&S	Image	Economics	Environment
H&S	1.00	0.3333	0.1111	0.3333
Image	3.00	1.00	0.1667	3.0000
Economics	9.00	6.00	1.00	7.0000
Environment	3.00	0.33	0.14	1.00
Weights	0.0534	0.1750	0.6667	0.1049

Consistency index	11.0814
Consistency ratio	12.3127

Performance Measures		
	Impact on Health and Safety	
	Long-term Impact	Immediate Casualties
Long-term Impact	1.00	4.00
Immediate Casualties	0.25	1.00
Weights	0.8000	0.2000

	Impact on Image		
	Internal	General Public	Customers
Internal	1.00	0.33	0.11
General Public	3.00	1.00	0.13
Customers	9.00	8.00	1.00
Weights	0.0675	0.1463	0.7861

Consistency index	10.7631
Consistency ratio	18.5570

	Impact on Economics	
	Own	External
Own	1.00	0.13
External	8.00	1.00
Weights	0.1111	0.8889

**Data from Decision Maker 3 (DM3):**

	Impact Categories			
	H&S	Image	Economics	Environment
H&S	1.00	0.3333	0.1429	0.2000
Image	3.00	1.00	0.1429	0.1429
Economics	7.00	7.00	1.00	1.0000
Environment	5.00	7.00	1.00	1.00
Weights	0.0580	0.0940	0.4396	0.4083

Consistency index	11.0647
Consistency ratio	12.2942

Performance Measures		
	Impact on Health and Safety	
	Long-term Impact	Immediate Casualties
Long-term Impact	1.00	7.00
Immediate Casualties	0.14	1.00
Weights	0.8750	0.1250

	Impact on Image		
	Internal	General Public	Customers
Internal	1.00	5.00	1.00
General Public	0.20	1.00	0.14
Customers	1.00	7.00	1.00
Weights	0.4353	0.0782	0.4866

Consistency index	0.8196
Consistency ratio	1.4131

	Impact on Economics	
	Own	External
Own	1.00	1.00
External	1.00	1.00
Weights	0.5000	0.5000

**Data from Decision Maker 4 (DM4):**

	Impact Categories			
	H&S	Image	Economics	Environment
H&S	1.00	0.3333	3.0000	0.1429
Image	3.00	1.00	5.0000	0.2000
Economics	0.33	0.20	1.00	0.1429
Environment	7.00	5.00	7.00	1.00
Weights	0.1057	0.2162	0.0547	0.6234

Consistency index	13.7255
Consistency ratio	15.2506

Performance Measures		
	Impact on Health and Safety	
	Long-term Impact	Immediate Casualties
Long-term Impact	1.00	7.00
Immediate Casualties	0.14	1.00
Weights	0.8750	0.1250

	Impact on Image		
	Internal	General Public	Customers
Internal	1.00	0.14	2.00
General Public	7.00	1.00	5.00
Customers	0.50	0.20	1.00
Weights	0.1580	0.7311	0.1109

Consistency index	10.6083
Consistency ratio	18.2903

	Impact on Economics	
	Own	External
Own	1.00	7.00
External	0.14	1.00
Weights	0.8750	0.1250

**Data from Decision Maker 5 (DM5):**

	Impact Categories			
	H&S	Image	Economics	Environment

H&S	1.00	5.0000	3.0000	5.0000
Image	0.20	1.00	0.2000	3.0000
Economics	0.33	5.00	1.00	5.0000
Environment	0.20	0.33	0.20	1.00
Weights	0.5143	0.1158	0.3045	0.0654

Consistency index	15.3272
Consistency ratio	17.0302

Performance Measures		
	Impact on Health and Safety	
	Long-term Impact	Immediate Casualties
Long-term Impact	1.00	5.00
Immediate Casualties	0.20	1.00
Weights	0.8333	0.1667

	Impact on Image		
	Internal	General Public	Customers
Internal	1.00	5.00	0.20
General Public	0.20	1.00	0.11
Customers	5.00	9.00	1.00
Weights	0.2157	0.0612	0.7231

Consistency index	10.1917
Consistency ratio	17.5719

	Impact on Economics	
	Own	External
Own	1.00	0.14
External	7.00	1.00
Weights	0.1250	0.8750

## Appendix D

### Scenarios Data:

Terrorist attack scenarios;

Scenario 1:

		Utility	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10	Node 11	Node 12	Node 13	Node 14
Weight	Constructed Scales For Safety & Health															
0.4286	Workers															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	1	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization.	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	1	1	1	1	0	1	1	0	1	1	1	1	1	1
			0	0	0	0	0.059	0	0	0.45	0	0	0	0	0	0
Weight																
0.0857	Public															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	1	1	1	1	0	1	1	0	1	1	1	1	1	1
			0	0	0	0	0.059	0	0	0.188	0	0	0	0	0	0
Weight	Constructed Scales For Image															
0.0250	Internal Image															
Level	Constructed Scale															
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.0000	0	0	0	0	0	0	0	1	0	0	0	0	0	0
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.4490	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.1318	0	0	0	0	1	0	0	0	0	0	0	0	0	0
1.00	Verbal enquiry from Eastern Region Governor	0.0444	1	1	1	1	0	1	1	0	1	1	1	1	1	1
0.00	No negative image	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			0.0444	0.044	0.044	0.044	0.132	0.044	0.044	1	0.044	0.044	0.0444	0.0444	0.044	0.044

Weight																
0.0071	Image with the General Public															
Level	Constructed Scale															
4.00	International interest from the media.	1.0000	0	0	0	0	0	0	0	1	0	0	0	0	0	1
3.00	Repeated appearance in the national media appearance in the international media.	0.4092	0	0	0	0	1	0	0	0	0	0	0	0	0	0
2.00	Repeated publication in the local media, appearance in the national media	0.1363	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Single appearance in the local media	0.0374	1	1	1	1	0	1	1	0	1	1	1	1	1	0
0.00	No negative image with the General Public	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			0.0374	0.037	0.037	0.037	0.409	0.037	0.037	1	0.037	0.037	0.0374	0.0374	0.037	1
Weight																
0.0838	Image with Customers															
Level	Constructed Scale															
4.00	Most critical customers upset	1.0000	0	0	0	0	0	0	0	1	0	0	0	0	0	1
3.00	Numerous letters from different customers	0.3905	0	0	1	0	1	1	1	0	0	0	0	1	0	0
2.00	Repeated verbal communications, few letters	0.1658	1	1	0	1	0	0	0	0	1	1	1	0	1	0
1.00	Few verbal communications	0.0573	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			0.1658	0.166	0.391	0.166	0.391	0.391	0.391	1	0.166	0.166	0.1658	0.3905	0.166	1
Weight																
0.0381	Constructed Scales For Economic Impact on Own Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	1	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	1	0	1	1	1	0	0	0	0	1	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	0	1	0	0	0	0	1	1	1	0	1	1
			0	0	0.37	0	0.37	0.37	0.37	1	0	0	0	0.3697	0	0
Weight																
0.2664	Economic Impact on Other People's Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	1	0	0	1	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	1	1	0	1	1	0	1	1	1	1	1	1
			0	0	0	0	0.37	0	0	0.37	0	0	0	0	0	0
Weight																
0.0654	Constructed Scales For Environment Impact on the Environment															
Level	Constructed Scale															
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Medium environmental damage, with some animals perishing. Eventually	0.2842	0	0	0	0	1	0	0	0	0	0	0	0	0	0

	reversible															
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems	0.0686	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0.00	No environmental impact	0.0000	1	1	1	1	0	1	1	0	1	1	1	1	1	1
			0.0000	0.0000	0.0000	0.0000	0.2842	0.0000	0.0000	0.0686	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

## Scenario 2:

		Utility	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10	Node 11	Node 12	Node 13	Node 14
Weight	Constructed Scales For Safety & Health															
0.4286	Workers															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization.	0.1881	0	0	0	0	0	0	0	0	0	1	0	0	0	0
1.00	A few persons require light treatment.	0.0591	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	0	1	1	1	1	1	1	1	1	0	1	1	1	1
			0.0591	0	0	0	0	0	0	0	0	0.1881	0	0	0	0
Weight																
0.0857	Public															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881	1	0	0	0	0	0	0	0	0	1	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			0.1881	0	0	0	0	0	0	0	0	0.1881	0	0	0	0
Weight	Constructed Scales For Image															
0.0250	Internal Image															

Level	Constructed Scale															
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.0000	1	0	0	0	0	0	0	0	0	1	0	0	0	0
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.4490	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.1318	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1.00	Verbal enquiry from Eastern Region Governor	0.0444	0	1	1	1	1	1	1	1	1	0	1	1	1	0
0.00	No negative image	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	0.0444	0.0444	0.0444	0.0444	0.0444	0.0444	0.0444	0.0444	1	0.0444	0.0444	0.0444	0.1318
Weight																
0.0071	Image with the General Public															
Level	Constructed Scale															
4.00	International interest from the media.	1.0000	1	0	0	0	0	0	0	0	0	1	0	0	0	1
3.00	Repeated appearance in the national media appearance in the international media.	0.4092	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Repeated publication in the local media, appearance in the national media	0.1363	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Single appearance in the local media	0.0374	0	1	1	1	1	1	1	1	1	0	1	1	1	0
0.00	No negative image with the General Public	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	0.0374	0.0374	0.0374	0.0374	0.0374	0.0374	0.0374	0.0374	1	0.0374	0.0374	0.0374	1
Weight																
0.0838	Image with Customers															
Level	Constructed Scale															
4.00	Most critical customers upset	1.0000	1	0	0	0	0	0	0	0	0	1	0	0	0	1
3.00	Numerous letters from different customers	0.3905	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Repeated verbal communications, few letters	0.1658	0	1	1	1	1	1	1	1	1	0	1	1	1	0
1.00	Few verbal communications	0.0573	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	0.1658	0.1658	0.1658	0.1658	0.3905	0.1658	0.1658	0.1658	1	0.1658	0.1658	0.1658	1
Weight	Constructed Scales For Economic															



0.0381	Economic Impact on Own Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	1	0	0	0	0	0	0	0	0	1	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	0	1	1	1	1	1	1	1	1	0	1	1	1	0
			1	0	0	0	0	0	0	0	0	1	0	0	0	0
Weight																
0.2664	Economic Impact on Other People's Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	1	0	0	0	0	0	0	0	0	1	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	0	1	1	1	1	1	1	1	1	0	1	1	1	1
			0.3697	0	0	0	0	0	0	0	0	0.3697	0	0	0	0
Weight	Constructed Scales For Environment															
0.0654	Impact on the Environment															
Level	Constructed Scale															
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Medium environmental damage, with some animals perishing. Eventually reversible	0.2842	1	0	0	0	0	0	0	0	0	1	0	0	0	0
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems	0.0686	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No environmental impact	0.0000	0	1	1	1	1	1	1	1	1	0	1	1	1	1
			0.2842	0	0	0	0	0	0	0	0	0.2842	0	0	0	0

Scenario 3:

		Utility	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10	Node 11	Node 12	Node 13	Node 14
Weight	Constructed Scales For Safety & Health															
0.4286	Workers															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization.	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	0	0	0	1	0	0	0	0	1	0	0
0.00	No health impact	0.0000	1	1	1	1	1	1	0	1	1	1	1	0	1	1
			0	0	0	0	0	0	0.0591	0	0	0	0	0.0591	0	0
Weight																
0.0857	Public															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881	0	0	0	0	0	0	1	0	0	0	0	1	0	0
1.00	A few persons require light treatment.	0.0591	1	1	1	1	1	1	0	1	1	1	1	0	1	1
0.00	No health impact	0.0000	0	0	0	0	0	0	0.0757	0	0	0	0	0.0757	0	0
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight	Constructed Scales For Image															
0.0250	Internal Image															
Level	Constructed Scale															
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.0000	0	0	0	0	0	0	1	0	0	0	0	1	0	0
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.4490	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.1318	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Verbal enquiry from Eastern Region Governor	0.0444	1	1	1	1	1	1	0	1	1	1	1	0	1	1
0.00	No negative image	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			0.0444	0.0444	0.0444	0.0444	0.0444	0.0444	1	0.0444	0.0444	0.0444	0.0444	1	0.0444	0.0444
Weight																
0.0071	Image with the General Public															
Level	Constructed Scale															
4.00	International interest from the media.	1.0000	0	0	0	0	0	0	1	0	0	0	0	1	0	1
3.00	Repeated appearance in the national media appearance in the international media.	0.4092	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2.00	Repeated publication in the local media, appearance in the national media	0.1363	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Single appearance in the local media	0.0374	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image with the General Public	0.0000	1	1	1	1	1	1	0	1	1	1	1	0	1	0
			0	0	0	0	0	0	1	0	0	0	0	1	0	1
Weight																
0.0838	Image with Customers															
Level	Constructed Scale															
4.00	Most critical customers upset	1.0000	0	0	0	0	0	0	1	0	0	0	0	1	0	1
3.00	Numerous letters from different customers	0.3905	0	0	1	0	1	1	0	0	0	0	0	0	0	0
2.00	Repeated verbal communications, few letters	0.1658	1	1	0	1	0	0	0	1	1	1	1	0	1	0
1.00	Few verbal communications	0.0573	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			0.1658	0.1658	0.3905	0.1658	0.3905	0.3905	1	0.1658	0.1658	0.1658	0.1658	1	0.1658	1
Weight	Constructed Scales For Economic															
0.0381	Economic Impact on Own Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	1	0	0	0	0	1	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	1	0	1	1	0	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	0	1	0	0	0	1	1	1	1	0	1	1
			0	0	0.3697	0	0.3697	0.3697	1	0	0	0	0	1	0	0
Weight																
0.2664	Economic Impact on Other People's Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	0	0	1	0	0	0	0	1	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	1	1	1	1	0	1	1	1	1	0	1	1
			0	0	0	0	0	0	0.3697	0	0	0	0	0.3697	0	0
Weight	Constructed Scales For Environment															
0.0654	Impact on the Environment															
Level	Constructed Scale															
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Medium environmental damage, with some animals perishing. Eventually reversible	0.2842	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems	0.0686	0	0	0	0	0	0	1	0	0	0	0	1	0	0
0.00	No environmental impact	0.0000	1	1	1	1	1	1	0	1	1	1	1	0	1	1
			0	0	0	0	0	0	0.0686	0	0	0	0	0.0686	0	0

Machine failure scenarios;

Scenario 1: failure at link “e17”

		Utility	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10	Node 11	Node 12	Node 13	Node 14
Weight	Constructed Scales For Safety & Health															
0.4286	Workers															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	1	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization.	0.1881	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0.0591	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	0	1	1	1	1	1	1	1	1	1	1	1	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight																
0.0857	Public															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight	Constructed Scales For Image															
0.0250	Internal Image															
Level	Constructed Scale															
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.4490	0	0	0	0	0	0	1	0	0	0	0	0	1	0
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.1318	0	0	1	0	1	1	0	0	0	0	0	1	0	0
1.00	Verbal enquiry from Eastern Region Governor	0.0444	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	1	1	0	1	0	0	0	1	1	1	1	0	0	1
			0	0	0.1318	0	0.1318	0.449	0.449	0	0	0	0	0.1318	0.449	0
Weight																
0.0071	Image with the General Public															

Level	Constructed Scale															
4.00	International interest from the media.	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Repeated appearance in the national media appearance in the international media.	0.4092	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Repeated publication in the local media, appearance in the national media	0.1363	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Single appearance in the local media	0.0374	0	0	1	0	1	1	1	0	0	0	0	1	1	0
0.00	No negative image with the General Public	0.0000	1	1	0	1	0	0	0	1	1	1	1	0	0	1
			0	0	0.0374	0	0.0374	0.0374	0.0374	0	0	0	0	0.0374	0.0374	0
Weight																
0.0838	Image with Customers															
Level	Constructed Scale															
4.00	Most critical customers upset	1.0000	0	0	0	0	0	0	1	0	0	0	0	0	0	0
3.00	Numerous letters from different customers	0.3905	0	0	1	0	1	1	0	0	0	0	0	1	1	0
2.00	Repeated verbal communications, few letters	0.1658	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Few verbal communications	0.0573	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	1	1	0	1	0	0	0	1	1	1	1	0	0	1
			0	0	0.3905	0	0.3905	0.3905	1	0	0	0	0	0.3905	0.3905	0
Weight																
0.0381	Constructed Scales For Economic Impact on Own Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	0	0	1	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	1	0	1	1	0	0	0	0	0	1	1	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	0	1	0	0	0	1	1	1	1	0	0	1
			0	0	0.1311	0	0.1311	0.3697	0.3697	0	0	0	0	0.1311	0.1311	0
Weight																
0.2664	Economic Impact on Other People's Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight																
0.0654	Constructed Scales For Environment Impact on the Environment															
Level	Constructed Scale															
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Medium environmental damage, with some animals perishing. Eventually reversible	0.2842	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Minor, short term environmental impact.	0.0686	0	0	0	0	0	0	1	0	0	0	0	0	1	0

	No permanent damage to any ecosystems															
0.00	No environmental impact	0.0000	1	1	1	1	1	1	0	1	1	1	1	1	0	1
			0	0	0	0	0	0	0.0686	0	0	0	0	0	0.0686	0

## Scenario 2: Failure at Node 4 and link “e2”

		Utility	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10	Node 11	Node 12	Node 13	Node 14
Weight	Constructed Scales For Safety & Health															
0.4286	Workers															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization.	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	1	1	1	0	1	1	1	1	1	1	1	1	1	1
			0	0	0	0.0591	0	0	0	0	0	0	0	0	0	0
Weight																
0.0857	Public															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No health impact	0.0000	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight	Constructed Scales For Image															
0.0250	Internal Image															
Level	Constructed Scale															
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.4490	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.1318	0	0	1	1	0	0	0	0	0	0	0	0	1	0
1.00	Verbal enquiry from Eastern Region Governor	0.0444	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0.00	No negative image	0.0000	1	1	0	0	0	1	1	1	1	1	1	0	0	1

			0	0	0.1318	0.1318	0.0444	0	0	0	0	0	0	0	0.0444	0.1318	0
Weight																	
0.0071	Image with the General Public																
Level	Constructed Scale																
4.00	International interest from the media.	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Repeated appearance in the national media appearance in the international media.	0.4092	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Repeated publication in the local media, appearance in the national media	0.1363	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Single appearance in the local media	0.0374	0	0	1	1	1	0	0	0	0	0	0	1	1	0	0
0.00	No negative image with the General Public	0.0000	1	1	0	0	0	1	1	1	1	1	1	0	0	1	0
			0	0	0.0374	0.0374	0.0374	0	0	0	0	0	0	0	0.0374	0.0374	0
Weight																	
0.0838	Image with Customers																
Level	Constructed Scale																
4.00	Most critical customers upset	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Numerous letters from different customers	0.3905	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0
2.00	Repeated verbal communications, few letters	0.1658	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
1.00	Few verbal communications	0.0573	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	1	1	0	0	0	1	1	1	1	1	1	0	0	1	0
			0	0	0.3905	1	0.1658	0	0	0	0	0	0	0	0.1658	0.3905	0
Weight																	
0.0381	Constructed Scales For Economic Impact on Own Property																
Level	Constructed Scale																
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	0	0	0	1	1	1	1	1	1	0	0	1	0
			0	0	0.1311	1	0.1311	0	0	0	0	0	0	0	0.1311	0.1311	0
Weight																	
0.2664	Economic Impact on Other People's Property																
Level	Constructed Scale																
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight																	
0.0654	Constructed Scales For Environment Impact on the Environment																
Level	Constructed Scale																
3.00	Major Environmental Impact, with long-term damage to large, valuable ecosystems	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2.00	Medium environmental damage, with some animals perishing. Eventually reversible	0.2842	0	0	0	1	0	0	0	0	0	0	0	0	0	0
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems	0.0686	0	0	1	0	0	0	0	0	0	0	0	0	1	0
0.00	No environmental impact	0.0000	1	1	0	0	1	1	1	1	1	1	1	1	0	1
			0	0	0.0686	0.2842	0	0	0	0	0	0	0	0	0.0686	0

### Scenario 3: Failure at Node 9 and Node 3

		Utility	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10	Node 11	Node 12	Node 13	Node 14
Weight	Constructed Scales For Safety & Health															
0.4286	Workers															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization.	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	1	0	0	0	0	0	0	0	0	1	0	0
0.00	No health impact	0.0000	1	1	0	1	1	1	1	1	1	1	1	0	1	1
			0	0	0.0591	0	0	0	0	0	0	0	0	0.0591	0	0
Weight																
0.0857	Public															
Level	Constructed Scale															
4.00	A large share of the served population requires treatment	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Hundreds of persons require treatment, dozens of them hospitalization.	0.4499	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Dozens of persons require treatment, some of them hospitalization	0.1881	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	A few persons require light treatment.	0.0591	0	0	1	0	0	0	0	0	1	0	0	1	0	0
0.00	No health impact	0.0000	1	1	0	1	1	1	1	1	0	1	1	0	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight	Constructed Scales For Image															
0.0250	Internal Image															
Level	Constructed Scale															
4.00	Responsibility is taken away to Ministry of Interior/political instances	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	The Eastern Region Governor tightens control over JIC's operation and requires frequent reports.	0.4490	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	A written report is required by Eastern Region Governor/political instances to explain incidents	0.1318	0	0	1	0	0	0	0	0	1	0	0	0	0	0
1.00	Verbal enquiry from Eastern Region Governor	0.0444	0	0	0	0	0	0	0	0	0	0	0	1	0	0



0.00	No negative image	0.0000	1	1	0	1	1	1	1	1	0	1	1	0	1	1
			0	0	0.1318	0	0	0	0	0	0.1318	0	0	0.0444	0	0
Weight																
0.0071	Image with the General Public															
Level	Constructed Scale															
4.00	International interest from the media.	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Repeated appearance in the national media appearance in the international media.	0.4092	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Repeated publication in the local media, appearance in the national media	0.1363	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Single appearance in the local media	0.0374	0	0	1	0	0	0	0	0	1	0	0	1	0	0
0.00	No negative image with the General Public	0.0000	1	1	0	1	1	1	1	1	0	1	1	0	1	1
			0	0	0.0374	0	0	0	0	0	0.0374	0	0	0.0374	0	0
Weight																
0.0838	Image with Customers															
Level	Constructed Scale															
4.00	Most critical customers upset	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Numerous letters from different customers	0.3905	0	0	1	0	0	0	0	0	1	0	0	0	0	0
2.00	Repeated verbal communications, few letters	0.1658	0	0	0	0	0	0	0	0	0	0	0	1	0	0
1.00	Few verbal communications	0.0573	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No negative image	0.0000	1	1	0	1	1	1	1	1	0	1	1	0	1	1
			0	0	0.3905	0	0	0	0	0	0.3905	0	0	0.1658	0	0
Weight																
0.0381	Constructed Scales For Economic Impact on Own Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	1	0	0	0	0	0	1	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	1	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	0	1	1	1	1	1	0	1	1	0	1	1
			0	0	0.3697	0	0	0	0	0	0.3697	0	0	0.1311	0	0
Weight																
0.2664	Economic Impact on Other People's Property															
Level	Constructed Scale															
4.00	Dozens of Millions of Saudi Riyals	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3.00	Millions of Saudi Riyals	0.3697	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.00	Hundreds of thousands of Saudi Riyals	0.1311	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.00	Dozens of thousands of Saudi Riyals	0.0441	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No economic impact	0.0000	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			0	0	0	0	0	0	0	0	0	0	0	0	0	0
Weight																
0.0654	Constructed Scales For Environment Impact on the Environment															
Level	Constructed Scale															
3.00	Major Environmental Impact, with long-term damage to large, valuable	1.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	ecosystems															
2.00	Medium environmental damage, with some animals perishing. Eventually reversible	0.2842	0	0	1	0	0	0	0	0	1	0	0	0	0	0
1.00	Minor, short term environmental impact. No permanent damage to any ecosystems	0.0686	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.00	No environmental impact	0.0000	1	1	0	1	1	1	1	1	0	1	1	1	1	1
			0	0	0.2842	0	0	0	0	0	0.2842	0	0	0	0	0

## Appendix E

### Performance Index (PI) of PMCS for three scenarios for terrorist attack

scenario	Decision-Maker 1			Decision-Maker 2			Decision-Maker 3			Decision-Maker 4			Decision-Maker 5		
	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
PMCS	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI
Node1	0.0039	0.4152	0.0038	0.0243	0.5039	0.0233	0.0097	0.5165	0.0094	0.0114	0.4534	0.0055	0.0153	0.3237	0.0150
Node2	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
Node3	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
Node4	0.4075	0.0156	0.5527	0.5348	0.0972	0.6653	0.5205	0.0387	0.6380	0.3628	0.0456	0.3784	0.3134	0.0610	0.3995
Node5	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
Node6	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
Node7	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
Node8	1.1126	0.0266	1.0064	1.1737	0.1767	1.2256	1.1615	0.0684	1.1656	0.7755	0.0738	0.7228	0.8716	0.1104	0.7361
Node9	0.0993	0.0078	0.3623	0.1069	0.0486	0.5020	0.1109	0.0194	0.4361	0.0459	0.0228	0.3213	0.0634	0.0305	0.3037
Node10	0.0039	0.4636	0.0038	0.0243	0.5094	0.0233	0.0097	0.5230	0.0094	0.0114	0.4654	0.0055	0.0153	0.3790	0.0150
Node11	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
Node12	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
Node13	1.1400	0.9250	1.0327	1.3437	1.3114	1.3889	1.2293	1.1562	1.2314	0.8553	1.0497	0.7613	0.9784	0.8894	0.8410
Node14	1.1557	0.9435	1.0485	1.4832	1.4519	1.5293	1.2745	1.2051	1.2769	1.0275	1.2248	0.9394	1.0551	0.9682	0.9180
e1	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e2	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e3	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e4	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e5	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e6	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
e7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
e8	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
e9	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
e10	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e11	0.0039	0.4152	0.0038	0.0243	0.5039	0.0233	0.0097	0.5165	0.0094	0.0114	0.4534	0.0055	0.0153	0.3237	0.0150
e12	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e13	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e14	0.4075	0.0156	0.5527	0.5348	0.0972	0.6653	0.5205	0.0387	0.6380	0.3628	0.0456	0.3784	0.3134	0.0610	0.3995
e15	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e16	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
e17	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
e18	1.1126	0.0266	1.0064	1.1737	0.1767	1.2256	1.1615	0.0684	1.1656	0.7755	0.0738	0.7228	0.8716	0.1104	0.7361
e19	0.0993	0.0078	0.3623	0.1069	0.0486	0.5020	0.1109	0.0194	0.4361	0.0459	0.0228	0.3213	0.0634	0.0305	0.3037
e20	0.0039	0.4636	0.0038	0.0243	0.5094	0.0233	0.0097	0.5230	0.0094	0.0114	0.4654	0.0055	0.0153	0.3790	0.0150

e21	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e22	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e23	0.0039	0.4152	0.0038	0.0243	0.5039	0.0233	0.0097	0.5165	0.0094	0.0114	0.4534	0.0055	0.0153	0.3237	0.0150
e24	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e25	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e26	0.4075	0.0156	0.5527	0.5348	0.0972	0.6653	0.5205	0.0387	0.6380	0.3628	0.0456	0.3784	0.3134	0.0610	0.3995
e27	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
e28	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
e29	1.1126	0.0266	1.0064	1.1737	0.1767	1.2256	1.1615	0.0684	1.1656	0.7755	0.0738	0.7228	0.8716	0.1104	0.7361
e30	0.0993	0.0078	0.3623	0.1069	0.0486	0.5020	0.1109	0.0194	0.4361	0.0459	0.0228	0.3213	0.0634	0.0305	0.3037
e31	0.0039	0.4636	0.0038	0.0243	0.5094	0.0233	0.0097	0.5230	0.0094	0.0114	0.4654	0.0055	0.0153	0.3790	0.0150
e32	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e33	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e34	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e35	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e36	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211

### **Performance Index (PI) of PMCS for three scenarios for machine failure**

	Decision-Maker 1			Decision-Maker 2			Decision-Maker 3			Decision-Maker 4			Decision-Maker 5		
scenario	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
MCS	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI	PI
Node1	0.0039	0.4152	0.0038	0.0243	0.5039	0.0233	0.0097	0.5165	0.0094	0.0114	0.4534	0.0055	0.0153	0.3237	0.0150
Node2	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
Node3	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
Node4	0.4075	0.0156	0.5527	0.5348	0.0972	0.6653	0.5205	0.0387	0.6380	0.3628	0.0456	0.3784	0.3134	0.0610	0.3995
Node5	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
Node6	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
Node7	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
Node8	1.1126	0.0266	1.0064	1.1737	0.1767	1.2256	1.1615	0.0684	1.1656	0.7755	0.0738	0.7228	0.8716	0.1104	0.7361
Node9	0.0993	0.0078	0.3623	0.1069	0.0486	0.5020	0.1109	0.0194	0.4361	0.0459	0.0228	0.3213	0.0634	0.0305	0.3037
Node10	0.0039	0.4636	0.0038	0.0243	0.5094	0.0233	0.0097	0.5230	0.0094	0.0114	0.4654	0.0055	0.0153	0.3790	0.0150
Node11	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
Node12	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
Node13	1.1400	0.9250	1.0327	1.3437	1.3114	1.3889	1.2293	1.1562	1.2314	0.8553	1.0497	0.7613	0.9784	0.8894	0.8410
Node14	1.1557	0.9435	1.0485	1.4832	1.4519	1.5293	1.2745	1.2051	1.2769	1.0275	1.2248	0.9394	1.0551	0.9682	0.9180
e1	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e2	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e3	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e4	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366

e5	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e6	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
e7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
e8	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
e9	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
e10	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e11	0.0039	0.4152	0.0038	0.0243	0.5039	0.0233	0.0097	0.5165	0.0094	0.0114	0.4534	0.0055	0.0153	0.3237	0.0150
e12	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e13	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e14	0.4075	0.0156	0.5527	0.5348	0.0972	0.6653	0.5205	0.0387	0.6380	0.3628	0.0456	0.3784	0.3134	0.0610	0.3995
e15	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e16	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
e17	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
e18	1.1126	0.0266	1.0064	1.1737	0.1767	1.2256	1.1615	0.0684	1.1656	0.7755	0.0738	0.7228	0.8716	0.1104	0.7361
e19	0.0993	0.0078	0.3623	0.1069	0.0486	0.5020	0.1109	0.0194	0.4361	0.0459	0.0228	0.3213	0.0634	0.0305	0.3037
e20	0.0039	0.4636	0.0038	0.0243	0.5094	0.0233	0.0097	0.5230	0.0094	0.0114	0.4654	0.0055	0.0153	0.3790	0.0150
e21	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e22	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e23	0.0039	0.4152	0.0038	0.0243	0.5039	0.0233	0.0097	0.5165	0.0094	0.0114	0.4534	0.0055	0.0153	0.3237	0.0150
e24	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e25	0.1907	0.0078	0.4537	0.1652	0.0486	0.5603	0.2024	0.0194	0.5276	0.0690	0.0228	0.3444	0.0963	0.0305	0.3366
e26	0.4075	0.0156	0.5527	0.5348	0.0972	0.6653	0.5205	0.0387	0.6380	0.3628	0.0456	0.3784	0.3134	0.0610	0.3995
e27	0.0954	0.0071	0.0952	0.0826	0.0552	0.0816	0.1012	0.0200	0.1009	0.0345	0.0168	0.0286	0.0482	0.0341	0.0479
e28	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211
e29	1.1126	0.0266	1.0064	1.1737	0.1767	1.2256	1.1615	0.0684	1.1656	0.7755	0.0738	0.7228	0.8716	0.1104	0.7361
e30	0.0993	0.0078	0.3623	0.1069	0.0486	0.5020	0.1109	0.0194	0.4361	0.0459	0.0228	0.3213	0.0634	0.0305	0.3037
e31	0.0039	0.4636	0.0038	0.0243	0.5094	0.0233	0.0097	0.5230	0.0094	0.0114	0.4654	0.0055	0.0153	0.3790	0.0150
e32	0.0039	0.0039	0.0038	0.0243	0.0243	0.0233	0.0097	0.0097	0.0094	0.0114	0.0114	0.0055	0.0153	0.0153	0.0150
e33	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e34	0.0954	0.0039	0.3585	0.0826	0.0243	0.4787	0.1012	0.0097	0.4267	0.0345	0.0114	0.3158	0.0482	0.0153	0.2887
e35	0.2129	0.0039	0.0952	0.3454	0.0243	0.0816	0.3084	0.0097	0.1009	0.2824	0.0114	0.0286	0.2019	0.0153	0.0479
e36	0.5943	0.0227	1.0026	0.6757	0.1524	1.2022	0.7133	0.0587	1.1562	0.4203	0.0624	0.7173	0.3945	0.0951	0.7211

## Appendix F

Petrochemical Prices in US \$ (April 11, 2009)	
Ethylene	710 US \$\Ton
Propylene	860 US \$\Ton
Benzene	650 US \$\Ton
Styrene	1000 US \$\Ton
Methanol	230 US \$\Ton
MTBE	600 US \$\Ton
Polyethylene	1140 US \$\Ton
Polypropylene	1140 US \$\Ton
Polystyrnen	1110 US \$\Ton
PVC	690 US \$\Ton
MEG	540 US \$\Ton
PTA	850 US \$\Ton
Urea	280 US \$\Ton
Urea	260 US \$\Ton
Ammonia	270 US \$\Ton
Ammonia	265 US \$\Ton